# Cryptography and Competition Policy – Issues with 'Trusted Computing'

Ross Anderson

Cambridge University

**Abstract.** The most significant strategic development in information technology over the past year has been 'trusted computing'. This is popularly associated with Microsoft's 'Palladium' project, recently renamed 'NGSCB'. In this paper, I give an outline of the technical aspects of 'trusted computing' and sketch some of the public policy consequences.

## 1 Introduction

Customers of the computing and communications industries are getting increasingly irritated at ever more complex and confusing prices. Products and services are sold both singly and in combinations on a great variety of different contracts. New technology is making 'bundling' and 'tying' strategies ever easier, while IT goods and services markets are developing so as to make them ever more attractive to vendors. These trends are now starting to raise significant issues in competition policy, trade policy, and even environmental policy.

Ink cartridges for computer printers provide a good example. Printer prices are increasingly subsidised by cartridge sales: the combination of cheap printers and expensive cartridges enables vendors to target high-volume business users and price-sensitive home users with the same products. The level of cross-subsidy used to be limited by the availability of refilled cartridges, and cartridges from third-party aftermarket vendors. However, many printer cartridges now come with chips that authenticate them to the printer, a practice that started in 1996 with the Xerox N24 (see [5] for the history of cartridge chips). In a typical system, if the printer senses a third-party cartridge, or a refilled cartridge, it may silently downgrade from 1200 dpi to 300 dpi, or even refuse to work at all. An even more recent development is the use of expiry dates. Cartridges for the HP BusinessJet 2200C expire after being in the printer for 30 months, or 4.5 years after manufacture [3] – which has led to consumer outrage [4].

This development is setting up a trade conflict between the USA and Europe. Printer maker Lexmark has sued Static Control Components, a company making compatible cartridges and components, alleging that their compatible authentication chips breach the Digital Millennium Copyright Act [7, 6]. On February 27, 2003, Judge Karl Forester ordered Static Control to stop selling cartridges with chips that interoperate with Lexmark's printers pending the outcome of the case.

"The court has no trouble accepting SCC's claim that public policy generally favors competition," wrote Judge Forester. "The court finds, however, that this general principle only favors legitimate competition. Public policy certainly does not support copyright infringement and violations of the DMCA in the name of competition." So it would now appear that US law protects the right of vendors to use such market barrier technologies to tie products and control aftermarkets.

However, the European Parliament has approved a "Directive on waste electrical and electronic equipment" with the opposite effect. It is designed to force member states to outlaw, by 2006, the circumvention of EU recycling rules by companies who design products with chips to ensure that they cannot be recycled [8]. The scene looks set for yet another trade war between the USA and Europe. Which side should economists and computer scientists support?

Varian argues that tying printers to cartridges may be not too objectionable from a policy viewpoint [9]:

> The answer depends on how competitive the markets are. Take the inkjet printer market. If cartridges have a high profit margin but the market for printers is competitive, competition will push down the price of printers to compensate for the high-priced cartridges. Restricting after-purchase use makes the monopoly in cartridges stronger (since it inhibits refills), but that just makes sellers compete more intensely to sell printers, leading to lower prices in that market. This is just the old story of "give away the razor and sell the blades."

However, tying in other industries may well be:

> But if the industry supplying the products isn't very competitive, then controlling after-purchase behavior can be used to extend a monopoly from one market to another. The markets for software operating systems and for music and video content are highly concentrated, so partnerships between these two industries should be viewed with suspicion. Such partnerships could easily be used to benefit incumbents and to restrict potential entrants.

In a growing number of industries, technical tying mechanisms based on cryptography, or at least on software that is tiresome to reverse engineer, are being used to control aftermarkets:

- Mobile phone manufacturers often earn more money on batteries than on the sales of the phones themselves, so have introduced authentication chips into the batteries. A mobile phone may refuse to recharge an alien battery, and may turn up the RF transmitter power to drain it as quickly as possible. In Morotola's case, battery authentication was represented as a customer safety measure when it was introduced in 1998 [10];

– Carmakers are using data format lockout to stop their customers getting repairs done by independent mechanics. In the case of the writer's own car, for example, the local garage can do a perfectly adequate 10,000 mile service, but does not have the software to turn off the nagging 'service due' light on the dashboard. Congress is getting upset at such practices [12];
– Computer games firms have been using market barrier tricks for years. As with printers, the business strategy is to subsidise sales of the actual consoles with sales of the cartridges (or more recently, CDs) containing the software. Sales of accessories, such as memory cards, are also controlled, and there have been lawsuits invoking the DMCA against unlicensed accessory vendors. As with printers, laws are diverging; for example, it is legal to defeat the Sony Playstation's copy protection and accessory control mechanisms in Australia, but not in Canada [11].

Up till now, vendors wanting to introduce barrier technologies to control aftermarkets typically had to design them from scratch. It is hard to get security designs right first time – especially when the designers are new to information security technology – so most early designs were easily circumvented [1]. The legislative environment is uneven and unpredictable, as the above examples show. There are often major political issues, especially in industries that are already concentrated and exposed to regulation. So there are significant risks and costs associated with these barrier technologies, and they are by no means ubiquitous.

That may be about to change dramatically. The introduction of so-called 'trusted computing' will make it straightforward for all sorts of vendors to tie products to each other, to lock applications and data on different platforms, and to tie down licences for the software components of systems to particular machines. This is likely to usher in a significant change in the way in which many of the information goods and services industries do business, and may spill over into may traditional industries too. First, we need a brief overview of 'trusted computing'. (For more detail, see the Trusted Computing FAQ at [2].)

## 2 Trusted Computing

In June 2002, Microsoft announced Palladium, a version of Windows implementing 'trusted computing' and due for release in 2004. In this context, 'trusted' means that software running on a PC can be trusted by third parties, who can verify that a program running on a machine with which they are communicating has not been modified by the machine's owner. Programs will also be able to communicate securely with each other, and with their authors. This opens up a number of interesting new possibilities.

The obvious application is digital rights management (DRM): Disney will be able to sell you DVDs that will decrypt and run on a Palladium platform, but which you won't be able to copy. The music industry will be able to sell you music downloads that you won't be able to swap. They will be able to sell

you CDs that you'll only be able to play three times, or only on your birthday. This will be controversial; other applications will be less so. For example, trusted computing platforms can host games where cheating is much harder, or auction clients which can be trusted to follow a set of agreed rules – which will make it significantly easier to design many types of auction [13].

Palladium built on the work of the Trusted Computing Platform Alliance (TCPA) which included Microsoft, Intel, IBM and HP as founder members. The TCPA specification, version 1.0, was published in 2000, but attracted little attention at the time. Palladium was claimed to use TCPA version 1.1 which supports some extra hardware features, and the next generation of Pentium processors from Intel (the 'LaGrande' series), which offer an extra memory protection mode: the idea is that since many existing untrusted applications run with administrator privilege, that is in ring 0 of the processor, upgrading security without replacing all these applications requires yet another protected memory mode, called 'curtained memory', so that small parts of trusted software can run with extra privilege that gives them access to cryptographic keys. TCPA has recently been formally incorporated and relaunched as the 'Trusted Computing Group' [14].

The TCPA/TCG specifications set out the interface between the hardware security component (the 'Fritz chip'), which monitors what software and hardware are running on a machine, and the rest of the system, which includes the higher layers of software and the means by which the Fritz chips in different machines communicate with each other. Fritz's role in the 'trusted' ecology is to assure third parties that your machine is the machine you claim it to be, and that it is running the software that you claim it to be.

### 2.1 Terminology

There is some difficulty in finding a suitable name for the subject matter of this paper. Neither 'TCPA' nor 'Palladium' will really do. For a while, when public criticism of TCPA built up, Microsoft pretended that Palladium and TCPA had nothing to do with each other; this pretence was then abandoned. But as criticism of Palladium has increased in turn, Microsoft renamed it NGSCB, for 'Next Generation Secure Computing Base' [15]. Presumably this isn't the final name, and in any case it's a bit of a mouthful. We might refer to the project as 'trusted computing' but that has evoked principled opposition; Richard Stallman, for example, prefers 'treacherous computing' as the real purpose of the technology is to remove effective control of a PC from its owner. It is thus the opposite of trustworthy [16].

There is a further twist. In the information security community, the words 'trust' and 'trustworthy' have a more subtle meaning than in common parlance. The following example illustrates the difference. If an NSA employee is observed in a toilet stall at Baltimore Washington International airport selling key material to a Chinese diplomat, then (assuming his operation was not authorized) we can describe him as 'trusted but not trustworthy'. The proper definition is

that a *trusted* system or component is one whose failure can break the security policy, while a *trustworthy* system or component is one that won't fail [1]. Since this was pointed out, Microsoft has renamed 'trusted computing' as 'trustworthy computing' [17]. (Intel and IBM stick with 'trusted'.)

I will therefore refer to the subject matter as TC, which the reader can pronounce as 'trustworthy computing', 'trusted computing' or 'treacherous computing', according to taste. Perhaps in time we can arrive at a consensus on a more appropriate name (maybe 'controlled computing').

### 2.2 Control and governance

If the owner of a computer is no longer to be in ultimate control of it, then the big question is where the control goes. This is a question on which companies involved in TC have expressed different views at different times. A straightforward reading of the TCPA 1.0 specification suggests that a hierarchy of certification authorities would certify the various hardware and software components that could make up a TC system. The control would thus be exercised centrally by an industry consortium.

After the launch of Palladium, Microsoft took the public stance that there would be no mechanism in Palladium to support such central certification, and it would be up to the vendors of TC applications or of the content used by them to decide what combinations of hardware and operating system software would be acceptable. Thus, in the DRM case, it would be Disney – or perhaps Microsoft as the vendor of Media Player – who would certify particular platforms as being suitable for rendering 'Snow White'.

Further confusion has been created by the recent launch of Windows Server 2003, which contains some of the file locking functions previously ascribed to Palladium. A TC machine may therefore need a number of different layers of hardware and software to collaborate to provide the TC functionality: the curtained-memory CPU, the Fritz chip, the NGSCB software, the Windows 2003 (or later) platform, and the application.

This has enabled Microsoft to reply to early criticisms of TC saying that NGSCB will not do any of the bad things alleged of it; it will not censor your data or take away control of your computer. But Microsoft admits: 'It is true that NGSCB functionality can be used by an application (written by anyone) to enforce a policy that is agreed to by a user and a provider, including policies related to other software that the application can load' [18].

So the locus of trust is moved upwards in the stack, but it is not eliminated. This may be thought to make the competition policy issues less acute, but further reflection suggests that a competitor producing a GNU/linux platform running on TCPA hardware, and seeking certification for it, might have to get it approved by a large number of disparate content vendors in multiple jurisdictions, rather than simply bringing suit against a central certification authority run by an industry consortium. This does not imply that there will be no 'TC/linux' –

such a product is apparently being worked on by HP and IBM [19] – but it suggests that the competition between TC platforms may be less diverse than TC proponents claim. Even if it were a worthy goal to make DRM available on a large variety of platforms, this strategy of fragmenting control and making governance either diffuse or opaque promises to put up the per-platform entry costs to the point that only a small number of popular platforms are ever effectively supported, and that consumers will have little or no real choice.

There is slightly more clarity on the management of policy, by which we mean the rules that a particular application will enforce – such as tags for commercial CDs saying 'never copy' or 'one backup only', or for broadcast movies saying 'recording for time-shifted viewing allowed; copying not allowed'. The primary policy source will be a server at the application vendor, and there will be mechanisms for some policy to be devolved to system owners.

Thus, for example, a TC system used to enforce government-style protective markings for classified information may have a central policy that information may only move upwards, so that part of a 'confidential' file could be cut and pasted into a 'secret' file but not vice versa; there might be a further local policy component that would enable the author of a particular classified document to restrict it to a number of named individuals, or to prevent it from being forwarded, or to prevent it from being printed.

## 3 Value to corporate and government users

Using TC systems to protect classified government information and corporate secrets is an interesting application, and one being used to promote the TC agenda. "It's a funny thing," said Bill Gates. "We came at this thinking about music, but then we realized that e-mail and documents were far more interesting domains" [21].

Some details about how rights management mechanisms can be applied in this way to the control of confidential information, as opposed to things like music and video, have been released recently in a Microsoft paper on Windows Server 2003 [17]. (This anticipates the release of the full TC platform, but a number of the TC features have already appeared in early form in other Microsoft products; for example, the combination of trusted boot and software copy protection has turned up in the Xbox, albeit using primitive mechanisms that were readily circumvented [20]. The early releases of TC component technologies can at least give us some idea of likely mature functionality.)

The new features offered by Windows Server 2003 enable the creator of a document or other file to maintain some control over it regardless of where it may subsequently move. It will be possible to send an email with restrictions, such as that the recipient cannot forward it, or cannot print it, or can read it only if she has a 'secret' clearance, or that the document will only be readable until the end of the month. Apparently the new Windows software on each PC emulates the future role of the Fritz chip. Windows users who wish to use TC

functionality can then register, and an online service appears to be involved in deciding whether or not to make an appropriate decryption key available to the application. The details are not entirely clear at the time of writing.

Many government systems already have mandatory access controls that prevent any person or process reading a classified document unless they have an adequate clearance. The implementation of such systems is fraught with surprisingly many practical difficulties, described for example in [1]. The complexity of the information flows within real organisations tends to cause all the information to either float up to the highest level of classification, or float down to the lowest level; there is a tendency for the number of compartments in which information is held to become either unmanageably large, or so small as to give little protection against insiders; most applications have to be rewritten to deal with the increased complexity and restricted connectivity; and there are consistency problems when High and Low parts of the system acquire different views of the same data. In general, the experience of mandatory access control systems is that although they can prevent bad things from happening, they prevent even more good things from happening, and provide a poor ratio of benefit to cost. The trend in government systems nowadays is to use more lightweight mechanisms, coupled with procedural controls and disciplinary measures, to achieve the desired results, rather than expecting the technology to do all the work.

So it is unclear what value most of the proposed rights management mechanisms will bring to corporate and government users.

A restricted subset of them may well be adopted widely, though. One of the selling points of the technology is that a corporation can arrange for all internal emails to become unreadable after 90 days. Apparently, Microsoft already imposes such a discipline internally. Given the increasingly aggressive discovery tactics used in litigation, it is maybe rather attractive to corporate legal officers to make emails behave like telephone calls rather than like letters; whether this is in the public interest is, of course, another question.

Even such a simple application will turn out to be complex to implement, because of established policy conflicts. Export laws in many countries require companies to preserve copies of communications by which software, documentation or know-how on the dual-use list is exported; this may mean keeping all relevant emails for three years. Accounting regulations may require the preservation of relevant emails for six years. One can anticipate widespread tussles between policies mandating destruction, and policies mandating preservation. As with multilevel security policies, it may turn out to be very difficult to implement systems so that just the 'right amount' of data are preserved.

## 4 Value to content owners

There has been much lobbying by the content industry for stronger digital rights management systems, and for stronger legal protection for the systems that already exist. The argument is made that digital technologies allow free copying,

which will destroy content markets. This argument is less widely believed nowadays, as the means for copying CDs have been widely available for several years with no particularly noticeable impact on sales [22]. There are many factors from which the content industry can take comfort.

Swapping music informally is not free, because of the time and effort required to build social networks; peer-to-peer systems do not solve the problem, as they are poor at the critical functions of indexing and searching; any organised central index service, such as Napster, can be attacked by legal means; and the existing weak DRM mechanisms, such as those in Media Player, provide a high enough barrier for a number of music subscription services and e-book publishers to flourish. It is not at all clear that a much stronger DRM mechanism, such as that promised by TC, would provide substantial gains for the content owners over the emerging status quo [22].

It is argued by DRM proponents that stronger DRM will extend the reach of DRM solutions [19]. However, many of the benefits that have been talked about in this context are unlikely to yield viable business models. Enabling music lending, for example – the idea that you can lend your copy of a CD to a friend, with your own copy becoming unplayable until you get the main copy back – would enable people to implement a legal 'Napster' in which members' CD tracks were pooled, and were thus used very much more than the twice a year that an average CD is played. This seems unlikely to be attractive to the music industry. It may well be possible to practice more extreme forms of price discrimination if strong DRM is widely fielded. But it is unclear that most information businesses will get substantial benefit from perfect price discrimination, because of the transaction costs and the negative social externalities such as loss of privacy. In practice, the ability to differentiate three grades of product at three different prices seems to be adequate for most purposes [24].

There is also a significant risk – that if TC machines become pervasive, they can be used by the other side just as easily. Users can create 'blacknets' for swapping prohibited material of various kinds, and it will become easier to create peer-to-peer systems like gnutella or mojonation but which are very much more resistant to attack by the music industry – as only genuine clients will be able to participate. The current methods used to attack such systems, involving service denial attacks undertaken by Trojanned clients, will not work any more [23]. So when TC is implemented, the law of unintended consequences could well make the music industry a victim rather than a beneficiary.

There is a further risk, in that if Microsoft comes to control the electronic distribution of music and video content through a monopoly built on Media Player, then this could restrict competition in the content industries. For example, a small film producer in a minority language might find it even harder than at present to get effective distribution. The effects of this could be both economic and cultural. Certainly, many of the smaller firms in the content sector may find TC to be at best a mixed blessing.

In any case, if the music industry wants to provide more value for its customers, it is not at all clear that TC is a critical component. New and useful online services such as those supporting indexing, browsing and access to background information seem likely to increase the revenues from subscription as opposed to first-sale income, and thus decrease the industry's likely dependence on strong DRM.

## 5 Value to hardware vendors

Experience shows that security mechanisms often favour the interests of those who pay for them more than the interests of the customers for whose benefit they were putatively developed [1]. For example, the introduction of authentication and encryption into GSM mobile phones was advertised as giving subscribers greater security compared with analogue phones, which were easy to clone and to eavesdrop. However, more mature experience shows that the main beneficiaries were the phone companies who paid for the security development.

With the old analogue phones, people wanting to make free calls, or to defraud the system by calling 900 numbers controlled by associates, would clone phones, which would generally cost the phone companies money. With the GSM system, criminals either buy phones using stolen credit cards (dumping the cost on the banks) or, increasingly, use mobile phones stolen in street robberies (which cost the customers even more). As for privacy, almost all the eavesdropping in the world is performed by police and intelligence agencies, who have access to the clear voice data on the backbone networks anyway.

Such experience suggests that we examine the likely effect of TC on the business of its promoters.

In the case of Intel, the incentive for joining TCPA was strategic. As Intel owns most of the PC microprocessor market, from which it draws most of its profits, it can only grow if the PC market does. Intel has therefore developed a research program to support a 'platform leadership' strategy, in which they lead industry efforts to develop technologies that will make the PC more useful, such as the PCI bus and USB. Their modus operandi is described in [25]: they typically set up a consortium to share the development of the technology, get the founder members put some patents into a pool, publish a standard, get some momentum behind it, then license it to the industry on the condition that licensees in turn cross-license any interfering patents of their own, at zero cost, to all consortium members.

The positive view of this strategy was that Intel grew the overall market for PCs; the dark side was that they prevented any competitor achieving a dominant position in any technology that might have threatened their control of the PC hardware. Thus, Intel could not afford for IBM's microchannel bus to prevail, not just as a competing nexus of the PC hardware platform but also because IBM had no interest in providing the bandwidth needed for the PC to compete with high-end systems. The effect in strategic terms is somewhat similar to the old

Roman practice of demolishing all dwellings and cutting down all trees close to their roads or their castles. This approach has evolved into a highly effective way of skirting antitrust law. So far, the authorities do not seem to have been worried about such consortia – so long as the standards are open and accessible to all companies. The authorities may need to become slightly more sophisticated.

## 6 Value to software vendors

The case of Microsoft is perhaps even more interesting than that of Intel. In its original form, TCPA had the potential to eliminate unlicensed software directly: a trusted platform, reporting to a central authentication structure, could simply refuse to run unlicensed software. The mechanisms currently used to register software could be made very much harder to circumvent: the Fritz chip maintains a list of the hardware and operating system software components of a TC machine, and there is provision for these to be checked against positive and negative authorisation lists. The operating system can then perform a similar service for application programs. Among early TCPA developers, there was an assumption that blacklist mechanisms would extend as far as disabling all documents created using a machine whose software licence fees weren't paid. Having strong mechanisms that embedded machine identifiers in all files they had created or modified would create huge leverage. Following the initial public outcry, Microsoft now denies that such blacklist mechanisms will be introduced – at least at the NGSCB level [18][1].

The Palladium/NGSCB/Win2003 system as now presented relies on more subtle mechanisms. Control will not now, we are told, be exerted from the bottom up through the TC hardware, but from the top down through the TC applications. Walt Disney will be free to decide on what terms they will supply content to TC (and other) systems with particular configurations of hardware and software; if they decide to charge $12.99 for a DVD version of 'Snow White', $9.99 for a download for TC/Windows using Media Player, but refuse to to provide content for TC/linux at all, then Microsoft can claim, to the media and the antitrust authorities, that that is their decision rather than Microsoft's.

The resulting incentives run very strongly in Microsoft's favour. Given that TC/Windows will certainly be the dominant TC platform, most developers will make their products available for this platform first, and for others later (if at all) – just as most developers made their products available for Windows first and for Mac later (if at all) once it became clear that the PC market was tipping in the Wintel direction.

[1] It is of course hard to understand how, in the long term, Microsoft will refrain from moving against people who pirate its software, given that it can also do so at the Windows level, the application level, or through controlling interoperability between licensed and unlicensed platforms from the standpoint of licensed platforms.

So the antitrust concern should now focus not on Microsoft's control of Palladium/NGSCB, but rather on its control of the dominant applications – Media Player and Office.

### 6.1 The importance of applications

In effect, Microsoft is investing in equipping the operating system platform (NGSCB and Windows2003+) with TC mechanisms in order to reap a reward through higher fee income from its applications. This can be direct (such as charging double for Office) or indirect (such as taking a percentage on all the content bought through Media Player). From the competition viewpoint, everything will hinge on how hard it is for other firms to make their applications and their content interwork with Microsoft's applications and content. Where rents can be charged, it is in Microsoft's interest to made this interoperability as difficult as possible.

If popular music subscription services employ Media Player, and Media Player eventually requires a TC platform, then subscribers may be faced with the need to migrate to a TC platform, or lose access to the music they have already stored. Of course, once the use of a TC application becomes widespread, with many users locked in, license compliance mechanisms can be implemented that will be about as hard to evade as the underlying technology is to break. The business model may then follow that pioneered by Nintendo and other game console makers, in which expensive software subsidises cheap hardware. NGSCB/Palladium will then just be a subsidised enabling component, whose real function is to maximise revenue from high-price products such as Office, games and content rental.

If some set of mandatory access controls for email become a popular corporate application under Windows 2003, and mandatory access controls eventually require a TC platform, then corporate users may also have little choice but to migrate. In fact, they may have even less choice than music subscribers. Music fans can always go out and buy new CDs, as they did when CDs replaced vinyl; but if many corporate and official communications and records come to be protected using cryptographic keys that cannot conveniently be extracted from embedded mandatory access control mechanisms, then companies may have no choice at all but to follow the TC mechanisms that protect and control these keys.

### 6.2 Switching costs and lock-in

The role of switching costs in the valuation of information goods and services companies has been recognised over the last few years. In industries dominated by customer lock-in – such as the software industry – the net present value of a company's customer base is equal to the total switching costs involved in their moving to a competitor [24]. If it were more than this, it would be worth a competitor's while to bribe them away. If it were less, the company could simply put up its prices.

One effect of TC is to greatly increase the potential for lock-in. Suppose for example that a company information systems manager wants to stop buying Office, and move his staff to OpenOffice running on a GNU/Linux platform. At present, he has to bear the costs of retraining the staff, the cost of installing the new software, and the cost of converting the existing archives of files. There will also be ongoing costs of occasional incompatibility. At present, economic theory suggests that these costs will be roughly equal to the licence fees payable for Office.

However, with TC, the costs of converting files from Office formats to anything else may be hugely increased [26]. There may simply be no procedure or mechanism for export of TC content to a non-TC platform, even where this is fully authorised by the content owner. If the means for such export do exist, they are unlikely to be enough on their own if TC mandatory access control mechanisms become at all widely used. This is because much of the data in a company's files may come to be marked as belonging to somebody else.

For example, a law firm may receive confidential client documents marked for the attention of a named set of partners only. The law firm might feel the need to retain access to these documents for six years, in case they had to defend themselves against allegations of malpractice. So they would have to get their client's permission to migrate the document to, say, a TC/linux platform running OpenDRM and OpenOffice. A firm of any size will acquire thousands of business relationships, some of which go sour; even if the logistics and politics of asking counterparties for permission to migrate documents were acceptable, a number of the counterparties would almost certainly be uncooperative for various reasons. Like it or not, the firm would be locked into maintaining a TC/Windows environment as well as the new one[2]. Many similar scenarios can be constructed.

There are soft effects as well as hard ones. For example, controversy surrounding the whole TC initiative can increase uncertainty, which in turn can lead businesses and consumers to take the view 'better the devil you know'. The result can be an increase in switching costs beyond even that following from the technology. (Old-timers will recall the controveries over the 'fear, uncertainty and doubt' element in IBM's marketing when IBM, rather than Microsoft, ruled the roost.)

### 6.3 Antitrust issues

There is thus a clear prospect of TC establishing itself using network effects, and of the leading TC application becoming in practice impossible for a competitor to challenge once it has become dominant in some particular sector.

This will shed a new light on the familiar arguments in information industry antitrust cases. Competition 'for the market' has been accepted by many

[2] In fact, from the professional practice viewpoint, accepting restricted documents seems to be very hazardous. For example, what if the named partners with access to the documents leave or die?

economists of the information industries as being just as fair as competition 'within the market', especially because of the volatile nature of the industry, and the opportunities created every few years for challengers as progress undermines old standards and whole industry sectors are reinvented. But if the huge and growing quantities of application data that companies and individuals store can be locked down, in ways that make it in practice impossible for the incumbents to be challenged directly, this argument will have to be revisited.

In any case, the commercial incentive for Microsoft is clear. The value of their company should be roughly equal to the costs incurred – directly or indirectly – if their customers switched to competitors. If switching can be made twice as hard, then the value of Microsoft's software business should logically double.

There are further issues. Varian has already pointed out that TC can reduce innovation, by restricting the technical opportunities to modify existing products [9]; things will become even worse once application data are locked down. At present, many software startups manage to bootstrap themselves by providing extra ways of using the existing large pools of application data in popular formats. Once the owners of the original applications embrace TC, there will be every incentive for them to charge rentals for access to this data. This looks set to favour large firms over small ones, and incumbents over challengers, and to stifle innovation generally.

Other software application vendors will face not just the threat of being locked out from access to other vendors' application data, but also the prospect that if they can establish their product and get many customers to use it for their data, they can use the TC mechanisms to lock these customers in much more tightly than was ever possible by using the old-fashioned mechanisms of proprietary data formats and restrictive click-wrap contracts. This will open the prospect of much higher company valuations, and so many software vendors will come under strong pressure to adopt TC. The bandwagon could become unstoppable[3].

Some specific industry sectors may be hard hit. Smartcard vendors, for example, face the prospect that many of the applications they had dreamt of colonising with their products will instead run on TC platforms in people's PCs, PDAs and mobile phones. The information security industry in general faces disruption as many products are migrated to TC or abandoned.

The overall economic effects are likely to include a shift of the playing field against small companies and in favour of large ones; a shift against market entrants in favour of incumbents; and greater costs and risks associated with new business startups. One way of looking at this is that the computer and communications industries will become more like traditional industry sectors

[3] There does, of course, linger some doubt about the extent to which Microsoft, Intel and the other TC core members may retain some residual control over the TC mechanisms, which might be used to the detriment of a new TC-using company that came to be seen to pose a threat to platform dominance as Netscape did.

such as cars or pharmaceuticals. This may turn out to be a decidedly mixed blessing.

## 7 Conclusion and Scope for Future Work

For many years, security engineers have complained that neither hardware nor software vendors showed much interest in building protection into their products. Early work in security economics now suggests why this was so [27]. The high fixed costs, low marginal costs, high switching costs and network effects experienced by many IT firms lead to dominant-firm industries with strong first-mover advantages. Time-to-market is critical, and so the 1990s Microsoft philosophy of 'we'll ship it on Tuesday and get it right by version 3' was completely rational. Also, when competing to dominate a network market, firms have to appeal to the vendors of complementary goods and services. So operating system vendors have little incentive to offer complex access control mechanisms, as these simply get in the way of application developers. The relative unimportance of the end users, compared to the complementers, lead firms to adopt technologies (such as PKI) which cause application vendors to dump security and administration costs on to end users. Control of the application programming interface is critical to a platform owner, so best make it proprietary, complicated, extensible and thus buggy. It is much more important to facilitate price discrimination than to facilitate privacy. Finally, in the absence of wide knowledge of security, the lemons effect caused bad products to drive out good ones anyway.

What should have suddenly changed Microsoft's mind?

A cynic might argue that the recent Department of Justice antitrust settlement binds Microsoft to sharing information about interfaces and protocols except where security is involved. There is thus an incentive to rebrand everything the company does as being security-sensitive. Microsoft has also argued that recent publicity about network attacks of various kinds was a driver. However, Microsoft has already used obscurity of protocol design from time to time as a competitive tool. There is also a growing consensus that security scaremongering is getting out of hand to the point that average US business may be spending too much on information security rather than too little. Surely a worm or two a year cannot justify a significant change of policy and direction.

This paper argues that another important factor in the recent decision by Microsoft to spend nine-figure sums on information security, after virtually ignoring the issue for decades, is the prospect of increasing customer lock-in. (It should be noted that Intel, AMD, IBM and HP are also making significant investments in TC, despite no immediate antitrust threats.)

There are many other issues raised by TC, from censorship through national sovereignty to the fate of the digital commons and the future of the free and open source software movement [2]. But while these issues also merit very serious consideration, they should not altogether deflect regulators and other policymakers from viewing TC developments through the lens of competition policy.

What should legislators and regulators do? Perhaps some useful precedents can be found in patent law. For years, an unlawful tying contract would invalidate a UK patent; if I had a patent on a flour milling process and licensed it to you on condition that you buy all your wheat from me, than by making that contract I made my patent unenforceable against you (or anyone else). At the very least, one might suggest that the legal protection apparently granted by the DMCA and the EUCD to TC mechanisms that claim to be enforcing copyright should be voided in the event that they are used for anti-competitive purposes, such as accessory control or increasing customer lock-in.

But how should a regulator differentiate between 'good' and 'bad' tying? After all, it is a well known proposition in undergraduate economics courses that price discrimination is often efficient.

We would suggest that this question may be one of the more urgent and interesting facing the economics community today. An analysis purely on innovation grounds may not be particularly useful: government-mandated interoperability would reduce the incentives for innovation by incumbents, so regulators would have to balance the costs to incumbents against the benefits to future challengers. As incumbents are more able to lobby than future challengers – who may not even exist yet – this is a difficult balance to manage politically.

As an alternative, we suggest the test for legislators to apply is whether TC mechanisms increase, or decrease, consumer surplus. This is also the test that the literature on abusive patent settlements would suggest [28]. Given the claims by TC supporters that TC will create value for customers, and the clear expectation that it will also create value for the vendors, and all the fog of impassioned argument about the rights and wrongs of digital rights management, perhaps the test of whether the consumers end up better off or worse off may be the most simple and practical way to arrive at a consistent and robust policy direction on TC.

**Acknowledgements:** I had useful feedback on this paper from Hal Varian, Andrew Odlyzko, Stephen Lewis, Alan Cox, Lucky Green, Richard Clayton and Rupert Gatti; from anonymous reviewers at the Workshop on Economics and Information Security; and from the audience at Johns Hopkins University, where I gave the 2003 Wenk Lecture on this subject. I have also had general discussions on TC issues with hundreds of people since the publication of [2].

## References

1. RJ Anderson, *'Security Engineering – a Guide to Building Dependable Distributed Systems'*, Wiley (2001) ISBN 0-471-38922-6
2. RJ Anderson, "TCPA/Palladium FAQ", at `http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html`
3. M Magee, "HP inkjet cartridges have built-in expiry dates – Carly's cunning consumable plan", The Inquirer, 29 April 2003, at `http://www.theinquirer.net/?article=9220`

4. "Ink Cartridges with Built-In Self-Destruct Dates", Slashdot, at http://slashdot.org/articles/03/04/30/1155250.shtml
5. "Computer Chip Usage in Toner Cartridges and Impact on the Aftermarket: Past, Current and Future", Static Control, Inc., at http://www.scc-inc.com/special/oemwarfare/whitepaper/default.htm
6. "Lexmark invokes DMCA in Toner Suit", Slashdot, at http://slashdot.org/article.pl?sid=03/01/09/1228217&mode=thread&tid=123
7. "Prepared Statements and Press Releases", Static Control, Inc., at http://www.scc-inc.com/special/oemwarfare/lexmark_vs_scc.htm
8. M Broersma, "Printer makers rapped over refill restrictions", ZDnet Dec 20 2002, at http://news.zdnet.co.uk/story/0,,t269-s2127877,00.html
9. HR Varian, "New Chips Can Keep a Tight Rein on Customers", New York Times July 4 2002, at http://www.nytimes.com/2002/07/04/business/04SCEN.html
10. "Motorola Announces Availability of New Wireless Phone Batteries for Increased Performance and Safety, Featuring New Hologram Design", Motorola Press Release, July 23, 1998; pulled after being referenced in [2]; now archived at http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/mototola_battery_auth.html
11. D Becker, "Sony loses Australian copyright case", on CNN.com, July 26 2002, at http://rss.com.com/2100-1040-946640.html?tag=rn
12. N Pickler, "Mechanics Struggle With Diagnostics", AP, June 24 2002; previously at radicus.net; pulled after being referenced in [2]; now archived at http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/car-diagnostics.html
13. LM Ausubel, P Milgrom, "Ascending Auctions with Package Bidding", 2002, at http://www.ausubel.com/
14. Trusted Computing Group, http://www.trustedcomputinggroup.org/
15. J Lettice "Bad publicity, clashes trigger MS Palladium name change", The Register, Jan 27 2003, at http://www.theregister.co.uk/content/4/29039.html
16. R Stallman, "Can you trust your computer?", at http://newsforge.com/newsforge/02/10/21/1449250.shtml?tid=19
17. Microsoft Corp., "Windows Server 2003", Feb 20, 2003, at http://www.microsoft.com/windowsserver2003/rm
18. J Manferdelli, "An Open and Interoperable Foundation for Secure Computing", in Windows Trusted Platform Technologies Information Newsletter March 2003
19. JS Erickson, "OpenDRM", at http://xml.coverpages.org/EricksonOpenDRM20020902.pdf
20. A Huang, "Keeping Secrets in Hardware: the Microsoft Xbox Case Study", May 26 2002, at http://web.mit.edu/bunnie/www/proj/anatak/AIM-2002-008.pdf
21. P Thurrott, "Microsoft's Secret Plan to Secure the PC", WinInfo, June 23, 2002, at http://www.wininformant.com/Articles/Index.cfm?ArticleID=25681
22. S Lewis, "How Much is Stronger DRM Worth?" at *Second International Workshop on Economics and Information Security*, at http://www.cpppe.umd.edu/rhsmith3/index.html
23. SE Schechter, RA Greenstadt, MD Smith, "Trusted Computing, Peer-To-Peer Distribution, and the Economics of Pirated Entertainment", at *Second*

*International Workshop on Economics and Information Security*, at http://www.cpppe.umd.edu/rhsmith3/index.html
24. C Shapiro, H Varian, *'Information Rules'*, Harvard Business School Press (1998), ISBN 0-87584-863-X
25. A Gawer, MA Cusumano, "Platform Leadership: How Intel, Microsoft, and Cisco Drive Industry Innovation", Harvard Business School Press (2002), ISBN 1-57851-514-9
26. J Brockmeier, "The Ultimate Lock-In", Yahoo News. Mar 12 2003, at http://story.news.yahoo.com/news?tmpl=story2&cid=75&ncid=738&e=9&u=/nf/20030312/tc_nf/20982
27. RJ Anderson, "Why Information Security is Hard – An Economic Perspective", in *Proceedings of the Seventeenth Computer Security Applications Conference* IEEE Computer Society Press (2001), ISBN 0-7695-1405-7, pp 358–365, at http://www.cl.cam.ac.uk/ftp/users/rja14/econ.pdf
28. C Shapiro, "Antitrust Limits to Patent Settlements", preprint, at http://faculty.haas.berkeley.edu/shapiro/settle.pdf