'Trusted Computing' and Competition Policy – Issues for Computing Professionals

Ross Anderson

Cambridge University

Abstract. The most significant strategic development in information technology over the past year has been 'Trusted Computing' (TC). In this paper, I give an outline of TC, and sketch some of the possible effects on the computing business and the people who work in it.

1 Introduction

One of the most complex problems facing computing professionals is coping with the pricing strategies used by suppliers to extract the last possible cent from their customer base. Dominant suppliers, such as Microsoft nowadays and IBM a generation ago, try to lock customers in to their architectures, so that control can be extended from one product to another. Many products work in cycles of 'bargains-then-ripoffs'; once you have committed your organisation to a particular smartcard, or accounting package, the prices mysteriously rise.

Product tying is another strategy, of which the ink cartridges for computer printers provide a good example. Printers are subsidised by cartridges: this combination 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 refilled and third-party cartridges. So 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].

Cartridge tying is now leading to trade conflict between the USA and Europe. In the USA, a court has granted the printer maker Lexmark an injunction preventing the sale of cartridges with chips that interoperate with Lexmark's printers. Meanwhile, the European Parliament has approved a "Directive on waste electrical and electronic equipment" which 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].

Aftermarket control and product tying are growing very rapidly and using all sorts of technical mechanisms. Mobile phone manufacturers often earn more

money from selling a battery than from the phone that uses it, so have introduced authentication chips that make it hard to use competitors' batteries [10]. Carmakers are using data format lockout to stop their customers getting repairs done by independent mechanics [12]. And computer games firms have for years been charging software developers royalties, that they use to subsidise the sales of consoles [11].

Are these good or bad for business? The answer, according to economists, is "It depends." Hal Varian argues that tying printers to cartridges may be not too objectionable from a policy viewpoint, because the printer market is still competitive, and so tying the sales of cartridges to printers just makes sellers compete more intensely to sell printers, leading to lower prices in that market [9].

However, where tying mechanisms can be used to link together two markets in which there is relatively little competition – say, the market for operating systems and the market for web servers – then this can cut choice and push costs up. This was one of the objections made on competition policy grounds to Microsoft Passport. Merchants who wished to use Passport were compelled to use Microsoft web servers too.

Complex pricing and aftermarket control may now become even easier for vendors to implement, thanks to the introduction of 'Trusted Computing' [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.

Palladium built on the work of the Trusted Computing Platform Alliance which included Microsoft, Intel, IBM and HP as founder members. AMD has now joined and it has been relaunched as the 'Trusted Computing Group' [13]. TCG proposes a redesign of the PC hardware, in which the CPU acquires an extra level of privilege (that allows processes to access memory barred even to an ordinary superuser) and a hardware security component (the 'Fritz chip'), which monitors what software and hardware are running on a machine. The Fritz chips in different machines can 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.

Not everyone accepts the name 'trusted computing' for this technology. Microsoft prefers to call it 'trustworthy computing': just because you trust a system, that does not necessarily make it trustworthy. 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'. (In fact, the NSA definition of a trusted system is 'a system that can break the security policy'.) At the other end of the debate, Richard Stallman of the Free Software Foundation prefers 'treacherous computing', as the real purpose of the TCG's technology is to remove effective control of a PC from its owner [15].

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.

2.1 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. The original TCPA 1.0 specification suggestsed a hierarchy of certification authorities to 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.

The current industry view is that it will 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 will be Disney – or perhaps Microsoft as the vendor of Media Player – who would certify particular platforms as being suitable for rendering 'Snow White'. 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' will ultimately flow from a server maintained at the application vendor.

3 Value to corporate and government users

Application security servers can specify a broad range of policies. So 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. But implementing one-way information flow controls properly is hard [1]; so it is unlikely that they will be the killer application for TC.

Using TC systems to protect corporate secrets the application now 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" [19]. A first implementation of rights management mechanisms that 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 Windows Server 2003 [16].

Windows Server 2003 enables 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. 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 a decryption key available to the application. (This was only just released at the time of writing and the details still have to be elucidated.)

One of the key selling points of the technology is that a corporation can arrange for all internal emails to become unreadable after 90 days. Microsoft already imposes such a discipline internally. Given the increasingly aggressive discovery tactics used in litigation, it may be attractive to some corporate legal officers to make emails behave like telephone calls rather than like letters.

But even such a simple application may be complex to roll out into the real world. A law firm may be reluctant to get instructions from a client in the form of an email that only one partner can read, that cannot be printed, and that will become completely unreadable after 90 days. How can the firm protect itself against malpractice litigation, and what guarantees are available to the other partners?

That is not all. 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 every IS manager knows, it is an absolute minefield to automate procedures that had previously avoided conflicts by leaving enough human discretion for the hard questions to be fudged.

4 Value to content owners

The music and film publishing industries have lobbied hard for mechanisms like TC, to support stronger digital rights management systems. They have already achieved stronger legal protection for existing systems. They argue that digital copying will destroy their business, but this argument is losing force now that copying CDs has been easy several years and there has been no particularly noticeable impact on sales. On a careful analysis, 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 [20].

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 [21]. So when TC is implemented, the law of unintended consequences could well make the music industry a victim rather than a beneficiary.

5 Value to hardware vendors

Experience shows that security mechanisms often favour the interests of those who pay for them rather 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, and this 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 intelligence agencies, who get clear voice data from 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 [23].

The positive view of this strategy was that Intel grew the overall market for PCs; the dark side was that they used patent pooling and mandatory cross-licensing agreements to prevent any competitor achieving a dominant position in any technology that might have threatened their control of the PC hardware. Cynics point out that Intel could not afford for IBM's microchannel bus to prevail: it was not just a competing nexus of the PC hardware platform, but 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. Intel's strategy approach has evolved into a highly effective way of skirting antitrust law.

6 Value to software vendors

The case of Microsoft is even more interesting. In its original form, TC had the potential to eliminate unlicensed software directly: a trusted platform, reporting to a central authorisation service, could simply refuse to run unlicensed software. The mechanisms used to register software could be made very much harder to circumvent: the Fritz chip maintains a list of the hardware and system software components of a TC machine, and there is provision for these to be checked online.

Following some public protest, Microsoft now says that no blacklist mechanisms will be introduced – at least at the operating system level [17]. The Windows 2003 system appears to rely on more subtle mechanisms. Control will not now, be exerted from the bottom up through the TC hardware, but from the top down through the applications. Disney will be free to decide on what terms they will supply content to systems with particular 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 other computer platforms 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 strongly in Microsoft's favour. If TC/Windows becomes the dominant platform, most developers will make their products available for it 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. It is hardly surprising that Apple is trying to beat Microsoft to the draw by launching its own media download service.

6.1 The importance of applications

Microsoft seems to be investing in equipping the operating system platform with TC mechanisms in order to reap a reward through higher 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. 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. The TC operating system features 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 mandatory access controls for email become a popular corporate application under Windows 2003, and these 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 records come to be protected using cryptographic keys, then companies may have little choice but to follow the 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 [22]. 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 [24]. 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 insist on the right to retain access to the documents for six years, in case they had to

defend themselves against allegations of malpractice. Such an agreement would be encoded in the rights management attributes of the document, and enforced using TC mechanisms. The access rules could then be overridden only by the owner of the document, that is, the person who created it.

So if the law firm wanted to migrate from Office and Windows to OpenOffice running on a future TC/linux platform, they would have to get their clients' permission to migrate all protected documents. 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.

There are soft effects as well as hard ones. For example, controversy surrounding TC 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. (Oldtimers 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 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 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 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]; and things will become 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 main 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.

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.

It is hard to find any exact historical analogies. Perhaps the closest is the switch from canals to railways in the 1830s. While anyone with a boat could haul freight on a canal, a railway is much more of a natural monopoly, and railways were objected to in such terms at the time. Now railways were by no means an economic disaster, but they did lead to concentrations of economic power and competition abuses that in turn led to anti-trust laws in some countries, and to the railways' being taken into public ownership in others.

Predicting long-term outcomes is hard, but in the short term it seems reasonable to expect that TC's economic effects are likely to include a tilt 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 such as cars or pharmaceuticals. This may turn out to be a decidedly mixed blessing.

7 What Does This Mean for IT Professionals?

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 [25]. 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. But surely a worm or two a year cannot justify such 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 the hard-nosed businessman will probably view TC through the lens of competition policy. The critical question is: 'How will this enable Microsoft to extract more money from me?' The answer, quite simply, is this: 'By locking you ever more tightly into using Microsoft platforms such as Office'.

What might 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.

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 [26]. Given the claims 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 customers end up better off or worse off may be the most simple and practical way to arrive at a consistent and robust policy direction.

More: This is a shortened version of a paper entitled *Cryptography and Competition Policy – Issues with 'Trusted Computing'* which can be found at `http://www.ross-anderson.com`.

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. Trusted Computing Group, `http://www.trustedcomputinggroup.org/`
14. 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`
15. R Stallman, "Can you trust your computer?", at `http://newsforge.com/newsforge/02/10/21/1449250.shtml?tid=19`
16. Microsoft Corp., "Windows Server 2003", Feb 20, 2003, at `http://www.microsoft.com/windowsserver2003/rm`

17. J Manferdelli, "An Open and Interoperable Foundation for Secure Computing", in Windows Trusted Platform Technologies Information Newsletter March 2003
18. 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
19. P Thurrott, "Microsoft's Secret Plan to Secure the PC", WinInfo, June 23, 2002, at http://www.wininformant.com/Articles/Index.cfm?ArticleID=25681
20. 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
21. 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
22. C Shapiro, H Varian, *'Information Rules'*, Harvard Business School Press (1998), ISBN 0-87584-863-X
23. A Gawer, MA Cusumano, "Platform Leadership: How Intel, Microsoft, and Cisco Drive Industry Innovation", Harvard Business School Press (2002), ISBN 1-57851-514-9
24. 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
25. 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
26. C Shapiro, "Antitrust Limits to Patent Settlements", preprint, at http://faculty.haas.berkeley.edu/shapiro/settle.pdf