In law we trust? Trusted Computing and legal responsibility for Internet security

Yianna Danidou and Burkhard Schafer

Abstract This paper analyses potential legal responses and consequences to the anticipated roll out of Trusted Computing (TC). It is argued that TC constitutes such a dramatic shift in power away from users to the software providers, that it is necessary for the legal system to respond. A possible response is to mirror the shift in power by a shift in legal responsibility, creating new legal liabilities and duties for software companies as the new guardians of internet security.

1 Introduction

Trusted Computing (TC), a project commenced by an industry organization known as the Trusted Computing Group (TCG), was set up to achieve higher levels of security for the information technology infrastructure. It was driven by the recognition that it is insufficient to rely on users taking the necessary precautions, such as regularly updated firewalls and anti-virus systems themselves. The notion of *’trust’* as used in this paper is not the sociological concept, but was taken from the field of trusted systems, that is systems that can be relied upon to perform certain security policies. Nonetheless, the outcome ultimately would be to allow the user to ”blindly trust” his computer again, without a constant need for self-monitoring. Prevention of Denial of Service (DoS) attacks, the performance of access control and monitoring and the achievement of scalability are just some of the numerous technical challenges that the current distributed systems need to overcome. A trusted environment

Yianna Danidou
Computer Science Department, Americanos College, 2 & 3 Omirou Avenue, P.O. Box 22425, 1521 Nicosia, Cyprus, and PhD candidate, School of Law, University of Edinburgh, e-mail: yianna.danidou@ac.ac.cy

Burkhard Schafer
SCRIPT, School of Law, University of Edinburgh, Old College Edinburgh, EH8 9YL, e-mail: B.Schafer@ed.ac.uk

must fulfil three basic conditions: protected capabilities; integrity measurement and integrity reporting, all creating and ensuring platform trust [4].

TCG is an alliance of promoters like AMD, Hewlett-Packard (HP), IBM, Intel Corporation, Microsoft, Sun Microsystems Incorporation and of contributors like Nokia, Fujitsu-Siemens Computers, Philips, Vodafone and many more. The project was targeted to allow the computer user to trust his own computer and for ”others” to trust that specific computer [15]. In a more intuitive way, as Ross Anderson [2] noted,

> TC provides a computing platform on which you cannot tamper with the application software, and where these applications can communicate securely with their authors and with each other.

A preliminary literature survey suggests that while computer scientists seem primarily concerned with the technical feasibility of implementing TC, legal academics have tended to concentrate on content control and privacy issues[1, 2, 3, 5, 6, 9, 11, 16, 17, 19, 20, 25, 27]. Neither group appears to be overly concerned with an analysis of the implications of the imposition of legal liability for failure within such a system, or potential responsibility for wider social and legal concerns to which they may give rise. If greater legal responsibility is placed upon hardware/software providers, this may have a significant impact upon the speed and scope of system roll-out, and may leave the system vulnerable to threats from market pressures. This paper will analyse how law and regulatory responses to TC can on the one hand address some of the widespread public concern about the technology, while on the other hand can create both incentives and disincentives for TC developers to take a greater share of the burden to secure the information infrastructure from malicious attacks.

2 The TC environment: Protecting the IT infrastructure

Attacks on computing infrastructure safety is an increasingly safety critical matter, as a large and vital number of system procedures depend on it. The weak spot in the defence against DoS attacks - an obvious technical challenge - is unsophisticated customers who forget updating their software. As software providers can increasingly take on this task on behalf of the end-user, there is increased pressure on big software companies to take on more of the responsibility for internet safety [8]. Consequently, software and hardware industries try to find ways to create more secure systems - like TC. The importance of the security of the information infrastructure has, belatedly, also been recognised by governments worldwide. In the UK, the House of Lords Select Committee on Science and Technology submitted in 2007 a comprehensive report on personal internet security [13], which identified not only a long list of current dangers, but also the key stakeholders and their respective responsibility for internet security. They conclude that:

> The current emphasis of Government and policy-makers upon end-user responsibility for security bears little relation either to the capabilities of many individuals or to the changing

> nature of the technology and the risk. It is time for Government to develop a more holistic understanding of the distributed responsibility for personal Internet security. This may well require reduced adherence to the ”end-to-end principle”, in such a way as to reflect the reality of the mass market in Internet services.

However, in its 2007 report, the House of Lords did not ask for a change in the attribution of legal liability to software vendors. In its follow-up report in 2008 [12], a much more aggressive stance towards the role of vendor liability was taken, and the Government was urged to raise the potential for substantive changes in the legal liability of software vendors for the safety of the internet both in the EU and internationally. With similar considerations also taking place elsewhere, the solution promoted by the TC community can also be seen as an attempt to pre-empt potential legislative imposition of liability - if industry is seen playing its part, governments may be more reluctant to impose new statutory burdens[1].

This paper proposes a new look at the interaction between internet security, trusted computing and legal liability. It is argued that even if technical solutions to internet security will decrease the pressure on governments to introduce new liability legislation, the shift of power and control away from the user to software providers will also change the legal landscape of liability and the attribution of legal responsibility, with or without new legislative initiatives.

TC is often seen as a threat to privacy, understood in its more common meaning as a political concept. It gives multinational companies access to information we would prefer to keep private. But following the analysis of reliance liability by Collins [7], it is argued that TC is intimately linked to a rather different understanding of privacy, one that software companies may well want to preserve. Privacy in the field of contract law is linked to, but different from, the political concept of privacy. Classical contract law embodied a notion of *’privacy’ (or privity)* of contract[2] This concept restricted heavily possible liabilities arising from contractual relations to the parties of the contract. More specifically, it meant two related things: - one that a contract is private between parties and the other that the individual does not owe legal obligations to associates. However, modern contract law recognises increasingly systematic exceptions to this principle. In particular, as Collins notes, *’reliance liability’* has increasingly been accepted as a conceptual foundation of both tort and contract law. In practical terms, this means that liability can be imposed between persons outside a contractual nexus if one of them relied reasonably on the performance of the other party. A typical example is the possible legal recognition of the interests of an employer who hired a person on recommendation of a third party. While there is no contractual relation between employer and recommender, legal systems are increasingly willing to conceptualise this relation as *quasi-contractual* and protect through the imposition of liability the reasonable expectation or reliance of the employer in the correctness of the recommendation. We will examine whether TC’s services can be understood in analogy to such a recommendation, whether as

[1] Parallel developments to this strategy can be found elsewhere, e.g. in the response of gun manufacturers to the thread of state imposed liability for misuse of guns by unauthorised users, by exploring the use of biometric devices that make this type of misuse impossible.

[2] For a comparative analysis see [23].

a result reliance liability should ensue, if TC promoters are aware of this possibility and whether they tend to take any action about the liability issue in general.

While delictual (reliance) liability is a paradigmatic example of the rebalancing between power and responsibility discussed in this paper, there are other possibilities on the horizon that are just as troublesome: at present, enforcement of internet law, both private and criminal, rest on the ability to create reliable and authentic (digital) evidence. The ”Trojan defence”, a claim that a third party had access to a suspect’s machine, is a notable threat to this precondition of enforceable internet law. However, TC would grant a much larger number of people remotely accessing people’s computers, potentially invalidating any evidence secured from the machine. Can the state impose the right type of standards on the TC providers, and enforce compliance, to counter this threat? Will on the substantive law side the fact that TC providers routinely gather data about illicit activities on customer’s computers carry also a legal obligation to act on this knowledge?

3 The TC Controversy

The proponents of TC suggest that TC promises to provide four crucial advantages: reliability, security, privacy and business integrity. Together these guarantee a system that will be available when in need, that will resist any attack once protecting the system itself and the data, that will give the demanded privacy to the user and finally that provides to businesses the ability to interact effectively with their customers. Also, TC could provide protection from viruses due to the fact that a check will be applied to all files trying to ”enter” the system. New applications will be structured to achieve protection while this means that TC could be used to restrict access to everything from music files to pornography to writings that criticize political leaders. As our last, and for the time being fictitious, example shows, this approach is not without controversy. Content-owning businesses may wish to prevent end-users from doing particular things with files e.g. ripping copyright music files; and employers may wish to control employees’ ability to access and/or distribute information across corporate networks, and so support this functionality. However, individuals are likely to have significant concerns about the effect of such technical solutions on their rights for privacy and freedom of speech. This may well lead possible buyers to refuse the purchase of TC systems [2].

There is also a significant risk in such a scenario of the promotion of anti-competitive behavior. The personal computing market already faces competitive failures caused by the domination of ”Wintel”; adding TC, where ’non-trusted’ computers and applications can be frozen out, and unauthorized files can be barred or deleted, without significant safeguards, may only make things worse [10, 22].

Given the foregoing, it is unsurprising that TC has given rise to a number of controversies between its proponents and opponents. This is due to the fact that the aim of TCG will provide more trustworthiness from the point of view of software vendors and the content industry, but there is a real danger that it will be perceived as less trustworthy by the users, despite an objective increase in security. There are two reasons for this. First, because of the perception of constant surveillance by software providers, that generates a persistent feeling of exposure. Second, because research into risk and risk perception shows that risks are perceived comparatively more serious when people do not feel in control. Even though statistically speaking air travel is more secure than driving a car, the lack of control that an air passenger experiences increases also the perception of being at risk. Similarly, TC requires the user to trust a third party, a ”pilot”. Consequently opponents say that cryptographic systems do not offer enough security for the computer and thus for the user, but instead provide vendors and technology companies with the freedom to make *”decisions about data and application that typically have been left to users”* [26]. Proponents state that the implementation and application of technologies that provide TC will increase users’ trust in their ability to protect their systems from malicious code and guard their data from theft.

Some harsh critics have emerged, who will not be easily won over. Richard Stallman, founder of the Free Software Foundation and creator of the well-known GPL open source license, is one such opponent to TC. He declares that ”treacherous computing”, as he brands TC, will allow content providers, together with computer companies to make the computers obey them, instead of the users. In other words, the *”computer will stop functioning as a general-purpose computer”* and *”every operation may require explicit permission”* [24]. Even when one does not buy this specific conspiracy theory, it does bring one of the problems with TC to the point: it signifies a dramatic shift in power away from the user towards the software providers, a shift to which the law ought to react by also shifting liability and more general legal responsibility.

Table 1 Brief overview of the TC controversy

Proponents	Opponents
TC will provide:	Concerns on:
• reliability • security • privacy • business integrity • protection • more trustworthiness • increment of user’s trust for protection	• invasion of privacy • breach of security • freedom of speech • non-trusted applications can be frozen out and unauthorized files can be remotely deleted • less trustworthiness due to: – constant surveillance by TC providers – lack of user control • user restrictions • loss of anonymity • mandatory use of TC technology to grant communication

4 Critisism of TC

A number of problems will arise from the adoption of TC technology. The foremost problems as stated by the opponents of TC are that sharing of content will be much more difficult due to the fact that TC will be used for what they term ”Digital Restrictions Management”, so that videos, music and other multimedia can be played only on a specified computer. Secondly, Digital Rights Management (DRM) will be used for email and documents, leading to documents and emails that will disappear, or will not be readable on certain computers. Restrictions in downloading and installing all types of software unless permitted by the TC technology may also cause problems. Critics also suggest that TC might threaten Open Source Software (OSS) development, as both OSS operating systems and applications may fail to be recognized as trustworthy by TC systems, which will then refuse to run them. In addition, programs that use TC when installed will be able to continually download new authorization rules through the Internet and impose those rules automatically. In such circumstances it is claimed, that computers may apply the new instructions downloaded, without notification, to such a degree that a user will no longer be able to fully interact with their computer [2, 24].

It is almost inevitable that TC will cause problems of incompatibility with legacy systems, both hardware and software. As a result, users (home or business) may find themselves at risk of ”forced upgrades” and lost data from old applications e.g. applications whose serial numbers have been removed from support schedules or blacklisted. For businesses the impact will also be on the economical area. The cost of any swapping between products plus the cost of training the employees for proper use of the new products will be extravagant [2]. Although this paper does not focus on this aspect of TC, this clearly has the potential to raise competition law issues - particularly where existing near-monopoly players such as Microsoft and Intel are involved [22].

Remote Censorship is another ”feature” that TC can provide. Applications that delete pirated music or other non-authenticated files via remote-control are possible. Anderson’s ”traitor tracing” applications that report files that are not authenticated in order to report the user and then remotely delete the files, are about to be applied in business models [2].

Interoperation with other products will be achieved only where the vendor wants it to be applied. Vendors have a very good reason as to why they would want the latter to happen: because then all buyers will purchase the same product from the same company - so that they can interoperate with each other - and therefore there will be a network effect. In such a market, the leading company may choose not to interoperate with other companies and thus locking all other companies outside this network and all the users inside it [10].

Opponents of TC have not been unaware of these implications, and some have claimed that the reason for Intel investing in TC was a *”defensive play”* [2]. By increasing market size, enlargement of the company will be achieved. Anderson points out that*”They were determined that the pc will be the hub of the future home* *network"* and that Microsoft's motivation was the economic enlargement by the cost created by switching software to any similar competitive products [2].

As a result of the short overview on the aforementioned issues, it is foreseeable that power is taken away from the user - i.e. user restrictions, loss of anonymity, mandatory use of the TC technology to grant communication with other networks and personal computers. Then again, the paper argues that this must be controlled and rebalanced by increasing the legal liability and responsibility of the TC providers for the favor of the user.

Summarizing the above-mentioned study concerning the critisim that has emerged from TC:

- Difficult sharing of content due to DRM
- Documents and email can be remotely deleted or unreadable
- Downloading and installing software restrictions
- Might constist a thread to OSS development
- User interaction problems
- Incompatibility with legacy systems
- High cost for swapping between products and employees' training
- Competition law
- Remote cencorship
- Interoperation with other products

5 Law addressing these ethical concerns

TC is characterised by a dramatic shift of power and control away from the human user to the software itself; power that is ultimately exercised by software providers. The overall argument we present in this paper, is that with such great powers, great responsibility will have to come (legally regulated). Governments (and citizens) will ultimately accede to this power shift, and the resulting dangers to values such as personal privacy and autonomy, only if there is a corresponding increase of responsibility on the side of the software provider.

5.1 Imposing 'reliance liability'

As an example of this rebalancing of power and responsibility, the paper aims to argue that the nature of TC lends itself to the imposition of reliance liability at some point in the future. TC becomes a guaranteed seal of approval on which third parties will increasingly rely. To the extend that TC providers anticipate this development at all, an insurance based solution seems likely to have the potential to further increase the digital divide.

We argue that TC has the potential to change radically the way we think about internet governance. It will shift the balance of power totally to commercial entities, more specifically to the members of the TCG. One argument of the paper is that the legal analysis of this shift has so far been very limited, and where it took place at all, has been highly selective. We also argue that the discussion so far has not taken account of the fact that a power shift of this magnitude will (or should) also result in a shift of responsibility, and ultimately liability, to the commercial entities. After describing such a theory of *'legal responsibility in an age of trusted computing'*, issues such as DRM and copyright will have to be revisited.

It is suggested that a possible outcome of greater legal responsibility, created either through the use of express warranties, or through implied terms imposed by the courts, is an increase in the cost of TC, as hardware and software producers seek to reduce their financial exposure via insurance. This in turn raises questions about the cost/benefit of TC systems to end-users, and whether the use of such systems would further exacerbate the 'digital divide' amongst end-users. The uncertainty about 'digital divide' issues is increased by the fact that in the literature, different players in the TC environment appear to have different end-user groups in mind. HP seems to be aiming TC at corporate users, whilst other companies such as Microsoft, with its Palladium initiative, seems to have wider aims. Will potential liability play as large, or perhaps a larger part in *determining the viability* of TC as copyright and privacy issues?

Liability for faulty software is an area of considerable legal controversy, not least because it remains unclear in UK law whether software is to be treated as a good, a service, or something else. The distinction is important because it determines the nature and scope of liability that can be implied into a contract, and also to some extent what can be legitimately excluded by contract. TC further complicates the issue because a failure in such a system may be hardware or software related. Hardware is clearly a good [3] - if software is deemed to be a service or sui generis in nature, this suggests that different components of the TC concept might be held to different standards.

In a TC world, my computer can "trust" other computers that identify themselves as "Trusted Computing", and in turn is trusted by them. If the system fails, two possible scenarios occur:

1. I behave less conscientiously, relying on the TC protection, and my economic interests are damaged (by downloading e.g. malware). This is primarily a contractual issue between me and the TC provider. However, a dimension of complexity is added by the fact that without TC, my computer may not be any longer functional as an internet enabled device (as other machines will not talk to it). This "must have" aspect of TC means that the scope to exclude contractually liability by the TC provider may well be limited under good faith rules.
2. Someone else, relying on my computer's certificate, downloads harmful software from me. Does this third party have any claims against *my* TC provider, given that he acted in reasonable reliance on the TC certificate?

It has been suggested in the past that it would be useful to apply pressure to software vendors to improve software security and to ensure that the software provides the security it should provide, and that if this is not the case, then purchasers should be able to sue the software vendors for any kind of harm caused by the use of their products. However, while the House of Lords report [13] does indeed suggest that this type of liability can play a role to incentivize software producers to develop more secure applications, so far there is no attempt made to attribute liability to software producers if they deliver software that is ”designed unsafe”. TC software would by design be more secure, but also ”warrant” this security explicitly. Potentially therefore, the law could create a counterproductive incentive structure: Software that is by design (relatively) unsafe might avoid liability for damage caused by malicious software, but the comparatively more secure TC could be held liable because its security is contractually and explicitly guaranteed.

Chandler [5] analyses two approaches where the law could intervene in the software development process to provide the standards that the end-user demands. The first approach is the use of regulations or laws to overcome market failures (i.e. where the market fails to put pressure on manufacturers to produce more secure software, such as in a monopoly situation) by mandating minimum security standards. The second approach is *”to impose liability for negligently-designed software”* [5] an approach that presents some advantages for example:

> software intended for use in conditions where design flaws may lead to substantial losses may be treated differently from software that does not present high risks. [5]

Chandler [5] notes that applying a negligence standard to software security might be a way forward, but specifically warns that taking that path might cause the software industry to take measures that while improving security could have other, less desirable implications (loss of consumer freedom and the implications for competition). She also clarifies (in the context of DDoS attacks) that, currently, purchasers may find it difficult to sue vendors for liability for damage caused by their product’s failure. Firstly, license terms disclaiming or limiting liability may affect possible lawsuits. Secondly, users may face counterclaims of contributory negligence if they did not maintain properly their security by patches or virus scanning.

5.2 Imposing the duty to preserve evidence

The literature review indicates that TC providers can identify computer crimes [2, 21] that fall under the UK Computer Misuse Act. This can be easily done through the tamper-resistant security chip that will be contained in the trusted computing platform. Trustworthiness verification will be performed from the operating system before execution from the client [18].

Moreover, Professor Zittrain speaking in images, has stated that the TC:

> ...will employ digital gatekeepers that act like the bouncers outside a nightclub, ensuring that only software that looks or behaves a certain way is allowed in. The result will be more

> reliable computing – and more control over the machine by the manufacturer or operating system maker, which essentially gives the bouncer her guest list. [28]

Given that the TC providers will have the control over the client machine, and will know about computer crime, this brings up the questions whether they should be responsible to mention this crime to the authorities and in addition whether they are responsible to ensure that any data recovered during an investigation of a customer's TC are not tarnished. From the above statement of [28] it is clear that the TC providers, will have the control over the machines, and they will be able to access the machines in any possible way. This raises a lot of issues, like privacy and the owner's reference on ”Trojan defense”.

Pleading the ”Trojan defense” has and will continue to be a legal issue, as long as there is lack in tracking and tracing cyber-attacks as Lipson stated .

> The lack of proven techniques for effectively and consistently tracking sophisticated cyber-attacks to their source (and rarely to the individuals or entities responsible) severely diminishes any deterrent effect. Perpetrators feel free to act with nearly total anonymity. [14]

This makes things worse, as with the TC platform, the group of people accessing the PC widens considerably to potentially any individuals within a TC organization that can legally or maliciously get access to the relevant control interfaces. Thus, the possibility and the danger for malicious intrusions will be larger and the legal tracking route will be more complicated.

Conversely, when a TC provider spots illicit software on its customer's computer, it might make them under some legal regimes complicit in the crime. From this point an issue arises; what is the legal obligation of the TC organization? There are in fact, two possible answers: either the TC provider informs the user and arrange the matter discreetly and unofficially, or the TC provider can report the illegal material.

6 Conclusions

The security of the communication infrastructure has belatedly gained by governments the interest that it deserves. In addition to the protection of safety critical infrastructure, consumers too need to be confident in internet security to allow digital economies to flourish. The House of Lords Report rightly criticized the UK government for over-emphasizing the responsibility of individual computer users. However, its main recommendation is a more prominent role of the state. TC offers an alternative, where security is not entrusted to the user, nor enforced by state sanctions, but embedded into the very fabric of the internet.

However, this would entail a dramatic *shift of power* away from consumers and state regulatory bodies to the software providers, a shift that has been described as unacceptable by many commentators. The argument that has been developed in this paper stated that such a shift can be justifiable, but only if it is accompanied by an equivalent shift in legal responsibility. With software providers taking on a role previously deemed to be the prerogative of the state (i.e. protection of crucial infrastructure), the user-TC relation needs to come closer to the citizen-state relation. Users will only accept TC as a technology that in fact infringes their autonomy if they can rely on robust legal safeguards if things go wrong. Imposing reliance liability is as we argued one well-established legal mechanism to address this power/responsibility shift that worked well in other fields of economic activity. But since it makes TC providers liable in tort for the proper functioning of user's computers also outside the contractual nexus (and hence outside their control) it may well increase the costs and decrease the incentives for TC development. Similarly, we argued that other legal duties previously associated with the state, such as the robust preservation of evidence in criminal proceedings and crime investigation more generally, may have in parts to be transferred to TC providers. So far, our research indicates that awareness of these possible developments in the TC community is low. They need to be raised to ensure that the costs, benefits and dangers can be properly quantified.

References

1. Anderson R (2003) Cryptography and Competition Policy Issues with 'Trusted Computing'. In: Proc of the twenty-second annual symposium on Principles of distributed computing (PODC '03). ACM, Boston, Massachusetts: 3–10
2. Anderson R (2003) Trusted Computing Frequently Asked Questions /TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA - Version 1.1. http://www.cl.cam.ac.uk/˜rja14/tcpa-faq.html. Cited 2 Oct 2008
3. Bradgate R (1999) Beyond the Millennium - The Legal Issues: Sale of Goods Issues and The Millennium Bug. JILT 1999(2). http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1999_2/bradgate/. Cited 2 Oct 2008
4. Burmester M, Mulholland J (2006) The advent of trusted computing: implications for digital forensics. In: Proc of the 2006 ACM symposium on Applied computing. ACM, Dijon, France: 283–287
5. Chandler JA (2003) Security in Cyberspace: Combating Distributed Denial of Service Attacks. UOLTJ 1(1-2):231–261
6. Charlesworth AJ (2005) DRM: the Straw to Break the Back of Procrustean Approaches to Copyright?. In: Grosheide FW and Brinkhof JJ (eds) Intellectual Property 2004, Articles on Crossing Borders between traditional and actual. Intersertia, Belgium: 405–422
7. Collins H (1987) The Decline of Privacy in Private Law. J Law Soc 14(1):91–103
8. Edwards L (2006) Dawn of the Death of Distributed Denial of Service: How to Kill Zombies. Cardozo AELJ 24(1):23–62
9. Erickson JS (2003) Fair use DRM and Trusted Computing. Commun ACM 46(4):34–39
10. Felten E (2003) Understanding Trusted Computing - Will Its Benefits Outweigh Its Drawbacks?. IEEE Security and Privacy 1(3):60–62
11. Hilley S (2004) Trusted computing - path to security or road to servitude?. Network Security 2004(8):12–15
12. House of Lords Publications (2008) In: Science and Technology - Fourth Report, Session 2007-08. House of Lords. http://www.publications.parliament.uk/pa/ld200708/ldselect/ldsctech/131/131.pdf. Cited 10 Dec 2008
13. House of Lords Publications (2007) In: Science and Technology - Fifth Report, Session 2006-07. House of Lords.

http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/16502.htm. Cited 13 Oct 2008

14. Lipson HF (2002) Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. In: University C M (ed) CERT Coordination Center, Special Report, CMU/SEI-2002-SR-009:49
15. Lohmann von F (2004) Meditations on Trusted Computing. In: Electronic Frontier Foundation, Whitepapers.
http://www.eff.org/wp/meditations-trusted-computing. Cited 10 Jan 2009
16. Pearson S (2005) Trusted Computing: Strengths, Weaknesses and Further Opportunities for Enhancing Privacy. In: Lecture Notes in Computer Science (ed) Trust Management. Springer, Berlin 3477/2005:305–320
17. Reid J, Nieto JMG, Dawson E et al (2003) Privacy and Trusted Computing. In: Proc of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03):383–388
18. Richardson R (2003) Eighth Annual 2003 CSI/FBI Computer Crime and Security Survey. In: Computer Security Institute.
http://www.gocsi.com. Cited 20 Oct 2008
19. Roemer R (2003) Locking Down Loose Bits: Trusted Computing Digital Rights Management and the Fight for Copyright Control on Your Computer. UCLA J of Law & Technology 8.
http://www.lawtechjournal.com/articles/2003/08_040223_roemer.php. Accessed 20 Oct 2008
20. Samuelson P (2003) DRM {and, or vs.} the Law. Commun ACM 46(4):41–45
21. Schell R, Michael F (2000) Platform security: What is lacking?. Information Security Technical Report 5(1):26–41
22. Schoen S (2005) Compatibility, competition, and control in Trusted computing environments. Information Security Technical Report 10(2):105–119
23. Snijders HJ (2007) Privacy of Contract. In: Studies - Oxford Institute of European and Comparative Law. Hart 2007(5):105–116
24. Stallman R (2002) Can you trust your computer?. In: NewsForge - The Online Newspaper for Linux and OpenSource.
http://www.newsforge.com/business/02/10/21/1449250.shtml?tid=19. Cited 15 Oct 2008
25. Turner M, Budgen D, Brereton P (2003) Turning software into a service. Computer 36(10):38–44
26. Vaughan-Nichols JS (2003) How Trustworthy is Trusted Computing?. Computer 36(3):18–20
27. Woodford C (2004) Trusted Computing or Big Brother? Putting the Rights back in Digital Rights Management. U Colo L Rev (75):253–300
28. Zittrain JL (2002) Taming the Consumer's Computer. In: The New York Times.
http://query.nytimes.com/gst/fullpage.html?res=990DEED81130F932A25750C0A9649C8B63. Cited 15 Oct 2008