BILETA
British & Irish Law, Education and Technology Association
2007 Annual Conference
Hertfordshire 16-17 April
UH

Legal Implications of Trusted Computing

Yianna Danidou
PhD Student, School of Law, University of Edinburgh
Email: I.Danidou@sms.ed.ac.uk

ABSTRACT

This paper reports the results of a research study carried out at the University of Bristol into the legal implications of trusted computing. The study combined empirical and socio-legal research with a conceptual evaluation of legal liability regimes. We will argue that the nature of Trusted Computing (TC) lends itself to the imposition of reliance liability at some point in the future. To the extend that TC providers anticipate this development at all, an insurance based solution seems likely that has the potential to further increase the digital divide.

Computers are becoming increasingly ubiquitous in our era, and their security and trustworthiness are vital to the development of electronic businesses and e-commerce. Data privacy, security from intrusions and malicious programs, and reliability in data protection, led required consideration of new ways to secure the computing environment. This is what "trusted systems" do. Trusted Computing (TC), a project commenced by an industry organization known as the Trusted Computing Group (TCG), was set up to achieve the aforementioned and to provide users with trusted systems.

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 [Lohmann 2003]. In a more explanatory way, as Ross Anderson noted "TC provides a computing platform on which you can't tamper with the application software, and where these applications can communicate securely with their authors and with each other"[Anderson 2003b].

Our aim is to examine the gap – identified through literature review – that lies between the current legal thinking about Trusted Computing – i.e. the exposure given to certain high-profile topics – and the lack of material on the public expectations that such a system may raise. We will focus on the legal liability of hardware and/or software companies in case of system failure, e.g. a security breach affecting end-users. In short, the focus is to examine the argument that while certain legal issues around Trusted Computing, like copyright, Digital Rights Management (DRM) and privacy, have been deeply discussed, the equally important question of liability appears to have been neglected.

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 Trusted Computing, as hardware and software producers seek to reduce their financial exposure via insurance. This in turn raises questions about the cost/benefit of Trusted Computing 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 Trusted Computing environment appear to have different end-user groups in mind. HP seems to be aiming Trusted Computing at corporate users, whilst other companies such as Microsoft, with its Palladium initiative, seems to have wider aims.

The research thus seeks to assess whether potential liability is likely to play as large a part, or perhaps a larger part, in determining the viability of Trusted Computing as technical feasibility, or copyright and privacy issues.

Our literature survey, suggests that while computer scientists seem primarily concerned with the technical feasibility of implementing Trusted Computing, legal academics have tended to concentrate on content control and privacy issues. 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. If greater liability 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.

Attacks on computing infrastructure safety is an increasingly safety critical matter, as a large and vital number of system procedures depend on it. Denial of Service (DoS) is one of the most obvious technical challenges that need to be defeated in order to achieve security for network infrastructure. The weak spot in the defence against DoS attacks are 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 the safety of the internet [Edwards 2006]. Consequently, software and hardware industries try to find ways to create more secure systems – like TC. One way of interpreting this move is 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. Parallel developments to this strategy can be found e.g. in the response of gun manufacturers to the thread of state imposed liability for misuse of guns by unauthorised users, exploring the use of biometric devices that make this type of abuse impossible. However, as we will argue below, such a move may well trigger much more far reaching reliance liability. Once monopolist institutions take on the job of dealing in security and make it factually impossible for private individuals to ensure their own security, there will be pressure on the legal system to protect the reliance of people on adequate delivery of this service even outside the scope of traditional contractual relations. Past developments of this nature in other fields have been well documented [Atiyah 1985]. For software producers, this poses an intricate dilemma: get too good at preventing attacks on internet infrastructure, and become de facto responsible for its smooth running. Leave it an essentially unstable environment, and face legislative action. To what extend do these legal challenges translate into design choices for TC? Or are there ways of avoiding both horns of the dilemma, and if so, who pays for the costs then?

Questions like these also allow us to approach the issue of privacy, the internet and TC from a new perspective. TC is primarily seen as a threat to privacy as a political concept, giving multinational companies access to information we would prefer to keep private. But following the analysis of reliance liability by Collins [Collins 1987], the issue is intimately lined to a rather different understanding of privacy, one that software companies may well want to preserve. Privacy in the field of contract law is inked to, but different from, the political concept of privacy. In contract y law, there are two notions of privacy – one that a contract is private between parties and the other that the individual does not owe legal obligations to associates. The first type of privacy, as Collins notes, had implications, which led to tort when manufacturers of defective products denied reliance on liability. Violation of the second notion of privacy however is what causes reliance liability, liability towards persons not party to the contract. As imposed by our hypothesis, we will examine whether TC's promoters are aware of this and whether they tend to take any action about the liability issue in general.

In order to assess the viability of our research to examine the liability hypothesis, a small-scale set of semi-structured interviews was conducted – the sample contained Hewlett Packard research staff members and Computer Science academic staff at the University of Bristol. The interviews uncovered a number of interesting issues, but also led to the conclusion that the issue is more complex to research than was originally expected.

INTRODUCTION TO TRUSTED COMPUTING

Prevention of denial of service, the performance of access control and monitoring and the achievement of scalability are just some of the numerous technical challenges that need to be overcome by the current distributed systems. These challenges concluded to the realization that system designers must proceed to the design of new systems that offer higher amount of trust than the currently implemented ones.

Trusted Computing (TC) is a project that was initially undertaken by the Trusted Computing Group (TCG) which 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 [Lohmann 2003]. In a more explanatory way, as Ross Anderson noted "TC provides a computing platform on which you can't tamper with the application software, and where these applications can communicate securely with their authors and with each other" [Anderson 2003b].

A trusted environment must fulfil three basic conditions: protected capabilities; integrity measurement; integrity reporting, all creating and ensuring platform trust [Burmester and Milholland 2006].

The Trusted Computing Group (TCG) is a non-profit corporate organization whose stated aim is "to develop, define and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals and devices" [TCG 2005].

TCG is headquartered in Portland, Oregon, but has an international membership. Currently the members are divided into three main hierarchical groups: at the top are the promoters – essentially the organizations that took the preliminary steps necessary for the formation of the corporation; contributors – organizations that contribute to the corporation; adopters – organizations that may adopt some of the technological outcomes of the organization. The last two groups currently number more than 130 members and TCG is still inviting active member participation [TCG 2006a][TCG 2006b].

Leading members (i.e. promoters) govern TCG via a board comprised of AMD, HP, IBM, Intel, Microsoft, Sony and Sun Microsystems. Members (i.e. contributors and adopters) cover a variety of companies drawn from areas like computing, software developers, systems vendors and network and infrastructure companies.

There are multiple areas in which TC promises significant impact. Regulated Endpoints and Distributed Firewalls is one of the applications that will be transformed by the use of TC. Customarily firewalls assume that everyone within the network is trusted, but whoever is outside it, is un-trusted. On the TC platform, "a distributed firewall is a significantly more powerful primitive since it can prevent packets that violate the central security policy from ever reaching the network in the first place" [Garfinkel *et al.* 2003]. Third Party computing is another application to be extended by TC. Today borrowing, leasing or donating computing resources is an everyday situation. Trusted platforms using attestation (mentioned above), can prove that they are running the expected executable file, and that the trusted operating system will keep the computation and its associated state private. The UK National Grid Service (NGS) is one such service that provides data resource access to UK academics to invigorate the use of e-Science resources and to impulse academics that never used grid computing resources to do so [NGS 2006].

Some other areas that have been, or have the potential to be, changed by TC are: Secure Infrastructure (Company Network), Secure Authentication (e-Banking), System Integrity, electronic cash, email, hot-desking, platform management, single sign-on, virtual private networks, Web access and digital content delivery [Pearson 2002].

TC can develop and promote open industry standards for hardware and software building blocks to enable more secure data storage, online business practices, and online commerce transactions while protecting privacy and individual rights.

The proponents of TC suggest that Trusted Computing promises to provide four crucial advantages: reliability, security, privacy and business integrity. Thus 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 will provide protection from viruses due to the fact that a check will be applied to all files trying to "enter" the system. This is to be done through structuring new applications that give new possibilities to the owners of computer systems and/or end users. One of them is that a TC system can detect files that are unauthorized, such as pirated music or software, or viruses and, delete them remotely. This means that TC could be used to restrict access to everything from music files to pornography to writings that criticize political leaders. This approach is not uncontroversial. Content-owning businesses may wish to prevent end-users 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 to purchase TC systems.

Given the foregoing, it is unsurprising that Trusted Computing has given rise to 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 will be less trustworthy from the point of view of their owners. Consequently opponents say that cryptographic systems don't 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" [Vaughan-Nichols 2003]. Proponents state that the implementation and application of technologies that provide trusted computing will increase users' trust in their ability to protect their systems from malicious code and guard their data from theft.

METHODOLOGY

Apart from literature search, we conducted some interviews, in order to address possible reasons for the literature gap identified. In our project we followed the 'criterion based' or 'purposive sampling' approach. Thus, the selection of the interviewees was criterion based. The sample of interviewees was chosen because of the knowledge and/or experience they had on the subject. Our general aim was to talk with people whose job involves interacting with issues about TC, either commercially, or academically and/or legally. Research staff at Hewlett Packard was chosen due to Hewlett Packard's direct relationship with the TCG and academic staff at the University of Bristol Department of Computer Science were chosen because of their particular knowledge about TC concepts.

MAIN FINDINGS

As mentioned in the abstract, while the literature search was progressing, a literature gap was identified. No one, neither in the computer science literature, nor in the legal literature seemed to have considered the issue of liability for the failure of a TC system. That is the issue of what happens if TC does not work the way it was planned to, or when trust is not provided to the user, in the way that a user defines "trust".

HP's researchers noted – while interviewing – that the research staff at HP Labs did not consider the liability issue in any depth, and suggested that HP's legal department would be better placed to come up with answers to those kinds of questions.

From the academic point of view, it was also commented that as far as computer science literature was concerned they hadn't seen any significant literature on the liability issue. Legal issues were not often seen as of great deal in the computer science field; although they felt the liability issue was an important issue that should be raised. Ross Anderson (an academic at the University of Cambridge Computer Laboratory) was mentioned during interviews; as an example of a computer scientist, who was deeply concerned with the legal issues relating to TC, but Anderson's interest was mostly focused in the areas of DRM and privacy and even he had not dealt with the liability side of TC.

The public's perception though, as discussed with HP staff members, is that when people hear "trusted platform" they tend to think that the platform must be secured so that is 100% trusted. The point that the researchers have made clear enough, is that when "trusted platform" comes up, doesn't mean that the platform can be 100% trusted, as unexpected things can happen to it, just as easily as with any application of this kind.

Furthermore, a "trusted platform", is a platform that helps the user to assess whether the connecting platform is secure or not, by using some primitive secure functions. The point of the platform being "trusted" is to detect whether there is something bad about the platform, and this is going to be revealed only if the platform has been asked the right questions. At the end of the day, the person using the trusted platform's information is the entity that will decide whether the other platforms communicating with theirs, is actually to be trusted or not.

Therefore, the mechanisms provided through the trusted platform are simply there to give information that help the end-user to decide whether the other platforms are trusted or not. It is most likely that the liability issue will be raised when the system that is sold to the public or to enterprises does not operate in the way expected, i.e. it doesn't function in the way the purchaser anticipated that it would, based on the information that they were given when deciding whether to purchase the system. It seems clear that the public's perception of TC and that which has gained common currency in the popular media of what a "trusted" system is, is not necessarily the one that at least some members of the TCG intended for "trusted computing".

As it seems from the lack of written material and from discussions we had with potential TC providers (i.e. HP), the issue of liability for failure of TC systems is either regarded as not a problem, or, alternatively that it is a problem of a different nature to that envisaged in the original hypothesis. It was certainly the case that both academic and industry interviewees saw a difference between the perspectives and understandings of ordinary pc end-users and those of corporate system purchasers. End-users are not so much of a problem, as they don't have the tendency to sue organizations over system failures. Businesses provide a bigger problem as they will go - and they have gone - to court in cases over the suitability of hardware and software for the purpose for which it had been sold.

As regards the question of liability, and the extent to which TC raises expectations amongst the public and especially in customers who might use systems incorporating the TC technology for mission critical applications, an academic interviewee made the case that vendors would be unlikely to be selling systems to business users on the basis that they were 'trusted systems'. Rather the systems would be sold on the basis of a specified quality of service that the vendor would be required to meet. Failure to meet that contractually specified level of quality of service would result in liability.

Thus, from the vendor's perspective the important issue is the extent of the risk they are expecting to assume in the process of promising the customer a specified level of service. If the level of risk is low enough, then the vendor may not take many precautions, as these would

probably not be cost effective, but if there is a higher level of risk, then this would make the use of additional technological solutions both viable and necessary. Such a solution might be to include TC components as a means of reducing the vendor's exposure to risk to that which can be readily managed or insured against. But what will actually be sold to the customer is a 'quality of service' warranty that the vendor believes its use of TC technology can sustain, and not a promise that the system can be 'trusted' because it contains TC technology.

Reinforcing this perspective, a researcher employed in one of the main players' organisations for the deployment of TC, said that TCG itself is not claiming to be designing a secure solution offered via TC, but instead is saying how this technology can be used to define primitive functions that will eventually provide a higher security level.

As a result, the TCG itself is not offering an overall security solution which might result in liability issues; it is only defining a protocol for obtaining information about the extent to which a computer might be trusted. Liability might arise from vendor-specific security solutions based on the information derived from the information from the primitive secured functions, but that would not be a direct result of the use of the TPM.

OUTCOMES

Following from the interviews, it was concluded that there was sufficient reason to believe that both academic and commercial researchers felt that the issue of liability in TC systems is an important, yet little discussed, issue. What was also clear, however, was that the liability issue as initially hypothesised was based on an interpretation of 'trusted system' that those interviewed were not convinced was the same as that envisaged by the TCG, although it might well have been in line with the public perception of the presentation of TC technology by the marketing departments of certain members of the TCG. It was felt that it would be necessary to reconsider the framing of the liability issue question, particularly in the light of the nature of 'quality of service' or 'service level agreement' arrangements common between vendors and enterprise level users. The role and scope of End-User Licence Agreements (EULAs) was also raised. These appear to work fairly effectively to limit software firms' liability for faulty software in the general user marketplace, or to at least dissuade members of the public from attempting to bring actions.

The question of whether the public perception of the reliability of computer hardware/software would be affected by the sale of systems containing TC components remained largely unresolved. As the literature review confirmed, no detailed examination of the issue has been raised or analysed in either the legal or computer science literature. Both commercial and academic researchers suggest that 'bug-free' software is unlikely without significant expenditure, which most users, both commercial and public, are unlikely to be inclined to pay. It is also clear, from a discussion we had with a possible TC vendor, that the initial premise raised here, that there might be a tension about the proper focus of liability, between software and hardware component providers in TC systems, is probably too simplistic. However, the question remains, if software manufacturers have, until now, been given a relatively easy ride by legislators and the courts on the basis that software cannot be fault free, it did not seem unreasonable that marketing 'trusted systems' or 'systems containing TC components' might affect the public perception of the fairness of that approach in apportioning risk between vendors and users.

With this in mind, the way that different parties interpret the concept of a "trusted" system is particularly interesting. The commercial researchers tended to argue that "trusted" doesn't mean that a system is invulnerable, merely that there are components within it which may allow the user to make a more informed decision about the 'trustworthiness' of a system or software. In that sense, they see a TC system as being potentially as vulnerable as any other. The key features that they see such systems providing are some help in providing higher security for a user's data and providing primitive security functions to help the user to assess whether a platform, should be trusted or not.

The academic interviewees were more likely to be sympathetic to a public perception of "trusted" as meaning that the actual platform must be trusted and secure and therefore if vulnerabilities come up, it should be able to handle them, even if they too were aware that this was not the underlying goal of the TCG.

The research undertaken demonstrated the extent to which legal issues other than liability had captured both media and academic attention. Both commercial and academic researchers were more at home in discussing the debates around issues such as DRM/copyright and privacy and were aware both of the arguments for and against TC in those scenarios, and of the negative publicity that such issues had provided for TC systems. In contrast, the issue of liability had been much less clearly thought through, and interviewees often seemed to be working out new angles on the liability question even as they were being interviewed. While most of the interviewees were not immediately convinced of the validity/applicability of the liability hypothesis being advanced in this research, they could see how the current development and marketing of TC systems might affect public perceptions about liability form provision of 'trusted systems' and possibly also for software provision generally.

REFERENCES

BOOKS

[Pearson *et al.* 2003] Balacheff, B., Cehn, L., Plaquin, D., Pearson, S. (ed.), and Proudler, G. (2003). *Trusted Computing Platforms - TCPA technology in context*, Hewlett-Packard Books.

[Atiyah 1985] Atiyah, Patrick: The Rise and Fall of Freedom of Contract (1985), *Oxford: Oxford University press*.

JOURNAL ARTICLES

[Vaughan-Nichols 2003] Vaughan-Nichols J. S. (2003). "How Trustworthy is Trusted Computing?" *IEEE Computer Society Press*, 36 (3), 18-20.

[Collins 1987] Collins, H. (1987) "The Decline of Privacy in Private Law" *Journal of Law and Society*, Vol. 14, No. 1, Critical Legal Studies (Spring, 1987), pp. 91-103.

[Edwards 2006] Edwards, L. (2006) Dawn of the Death of Distributed Denial of Service: How to Kill Zombies. *Cardozo Journal of Arts and Entertainment Law*, 24, (1), 23-62.

CONFERENCE PROCEEDINGS

[Anderson 2003a] Anderson, R. (2003) “Cryptography and Competition Policy Issues with ‘Trusted Computing’.” *Proceedings of the twenty-second annual symposium on Principles of Distributed Computing*, Boston, Massachusetts, 3-10.

[Burmester and Milholland 2006] Burmester, M., and Mulholland, J. (2006). “The advent of trusted computing: implications for digital forensics “ *Proceedings of the 2006 ACM symposium on Applied computing*, Dijon, France, 283 287.

[Garfinkel *et al.* 2003] Garfinkel, T., Rosenblum, M., and Boneh, D. (2003). “Flexible OS Support and Applications for Trusted Computing.” *Proceedings of HotOS’03: 9th Workshop on Hot Topics in Operating Systems*, 145 150.

PRESS RELEASES AND TECHNICAL REPORTS

[Pearson 2002] Pearson, S. (2002). Trusted Computing Platforms, the Next Security Solution, Prentice Hall PTR, Technical Report HPL-2002-221, HP Laboratories.

[TCG 2005] Trusted Computing Group (2005). "Fact Sheet.”

ELECTRONIC INFORMATION

[Anderson 2003b] Anderson, R. (2003). “Trusted Computing Frequently Asked Questions / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA – Version 1.1. (2003).” Available at: http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html (Copy on file with author).

[Lohmann 2003] Lohmann von F. (2003). “Meditations on Trusted Computing.”. Available at: http://www.eff.org/Infrastructure/trusted_computing/20031001_meditations.php. (Copy on file with author).

[NGS 2006] NGS. (2006). "National Grid Service.". Available at: http://www.grid-support.ac.uk/

[TCG 2006a] TCG. (2006). "Membership Levels." Available at: https://www.trustedcomputinggroup.org/join/levels/ .

[TCG 2006b] TCG. (2006). "Membership." Available at: https://www.trustedcomputinggroup.org/about/members/ .