Legal implications of Trusted Computing

Yianna Danidou
PhD Student, College of Humanities and Social Science – School of Law, University of Edinburgh
Email: yiannadanidou@gmail.com

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 2003].

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.

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.

References

[Anderson 2003] 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).