Ross Anderson, FIEE, FIMA
Reader, Security Engineering

Diana Alonso Blas, LL.M.
European Commission, DG Internal Market
Unit Media and Data Protection
Avenue de Cortenbergh 100, 6-31
B-1000 Brussels
Fax: 00-32-(2)2998094

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

July 24, 2003

Dear Diana,

Trusted Computing Group

Thank you for the opportunity to respond to the submission on data protection by the Trusted Computing Group.

The privacy objections to the program referred to by Intel as 'Trusted Computing', by Microsoft as 'Trustworthy Computing' and by the Free Software Foundation as 'Treacherous Computing' – and which I'll refer to simply as 'TC' – include the following.

First, TC will make it very much harder for PC users to detect and disable spyware. At present, many software companies put monitoring routines in their products, to measure some aspects of PC use and report it back over the Internet. There are also surveillance products spread by viral and other covert means. While some of these spyware products are lawful – for example, when used in court-mandated surveillance of criminal suspects – most feed information to marketers. While marketing surveillance products may be legal in the USA, many are of dubious legality in the EU.

At present, computer users can buy programs that detect and disable spyware. However, in the future, spyware authors will be able to use TC mechanisms to prevent the writers of anti-spyware programs from monitoring or interfering with their products. Furthermore, as TC mechanisms will be considered to be copyright protection mechanisms in terms of the EU Copyright Directive, the proposed Directive on IP Enforcement will compel all Member States to make it a criminal offence to interfere with TC mechanisms deliberately in the course of a business. Anti-spyware products will therefore be criminalised, and EU citizens will lack the means to defend themselves against probably unlawful privacy intrusions by US advertisers. For this reason, I strongly recommend that DG Internal Market push for the amendment of the draft Directive so that it gives legal protection to TC mechanisms only when they are being used for bona fide copyright protection; it should not extend the legal privileges of copyright into areas where lawmakers never intended to grant any privilege.

Computer Laboratory
JJ Thomson Avenue
Cambridge CB3 0FD
England

Tel: +44 1223 334733
Fax: +44 1223 334678
E-mail: Ross.Anderson@cl.cam.ac.uk

Second, TC will increase both the opportunity and the motivation for software vendors to extend price discrimination. While at present this is typically limited to having several versions of a software product, and perhaps offering educational discounts, TC is designed to support more sophisticated business models, such as application rental. Many of these models are more intrusive and the net effect will be to increase the collection of personal profile data, so that pricing decisions can be made more effectively. (See for example "The unsolvable privacy problem and its implications for security technologies", A. M. Odlyzko, at `http://www.dtc.umn.edu/~odlyzko/doc/research.html`.)

Third, TC will introduce a unique identifier into the PC world. The history of TC is that Intel decided in 1995 to introduce, quite unilaterally, mechanisms similar to TC into its processor chipsets by 2000 in order to support digital rights management (DRM). The first step on this path was the Pentium 3 serial number, launched in 1998. This caused a storm of protest in the USA on privacy grounds, which in turn led Intel to set up the Trusted Computing Platform Alliance (TCPA) which has now evolved into the TCG. Intel appears to have thought that with a broad industry alliance, and more skilful PR, the privacy objections can be sidelined. However, the arguments against mandatory unique PC identifiers remain.

At present, the typical PC contains a number of identifying numbers – its ethernet address, the serial number of the hard disk controller, and so on – but these change over time as machines are upgraded, and there is therefore no industry consensus on how to identify a platform. Introducing a universal identifier – as was proposed with the Pentium 3 serial number, and is now proposed with TC – will break this logjam and lead to software products logging machine identities in transaction data. Thus a document will likely have embedded in it the identifiers of all machines on which it had been edited, and banking transactions will contain the serial numbers of machines through which they have passed. This will enable third parties to correlate records much more precisely across domains.

For example, the UK proposes to build a huge central database of all medical records, which will have patient names removed to protect privacy, and will be used inter alia for research and administration. If the records in this database come to contain machine identifiers, then they might be matched against public data – such as the identifier in a word-processing document written and published by a patient. The privacy risks are clear; it was risks of this type that caused the outcry in the USA in 1998 and derailed the Pentium serial number project.

In an attempt to forestall such criticisms, TC supports pseudonyms. The owner can at any time decide that her existing machine identifier has received sufficient exposure, and generate a new one. There are mechanisms that will support a migration of protected data from the old identifier to the new one.

I do not believe that this proposed solution is even remotely adequate. The migration process will be tiresome, and some software vendors may refuse to cooperate – either for deliberate business reasons, or because they cannot be bothered to invest the extra programming effort to support migration. So it is likely that changing one's machine identity will be at best a tiresome process; at worst it may involve permanent loss of data such as one's song collection or part of one's document archive.

I turn now to the TCG's arguments.

1. TCG claims that TC is an opt-in technology that can be disabled by the user. One can equally argue that Windows is an opt-in technology; the user can always migrate to MacOS or GNU/Linux. Yet this did not stop Microsoft (the driving force nowadays in TCG) being convicted of antitrust law offences in the USA, nor the extensive competition policy case to which it's subject in the European Union. The simple fact is that network effects drive businesses to use Microsoft Office. Even academics have to use Microsoft Office – to get research grant funding from our national governments and from the EU! However much we use other systems, we need machines running Microsoft Office as well. Most home users have only a Windows machine; they cannot justify a second machine running exotic software. I refer you to Article 82 EU, on abuse of a dominant market position, and the legal opinion by Prof. Christian Koenig, "TCG und NGSCB auf dem Prüfstand des Wettbewerbsrechts", which can be found at `http://www.tkrecht.de/index.php4?direktmodus=vortraege`. (I'll return to cartel law issues later.)

2. The TCG quibbles about which monitoring functions are performed by the TPM and which by the Nexus – the TC component in the operating system. These quibbles are a distraction. They are taking issue with statements in my 'TCPA FAQ' which relate to the TCPA information made available as of May 2002. Since then, the TC specification has evolved from version 1.0 through 1.1 to 1.2, and the claimed size of the Nexus from 10,000 lines of code to 100,000 lines of code. Compared with the original public description of the technology, more functions will be performed in the Nexus, and fewer in the TPM.

   The ostensible reason for the change was that under TC version 1.0, a PC running a 'trusted' program and which started running an 'untrusted' one would have to abort the 'trusted' program and clear its memory. Thus no machine could run 'trusted' and 'untrusted' code simultaneously, which might have rendered the technology unusable in mass markets. Fixing this also entailed design changes in the CPU hardware – the forthcoming introduction of 'LaGrande Technology' in the next generation Pentium. So the changes since TCPA 1.0, and since I wrote the TPCA FAQ, have been extremely wide-ranging and are not yet fully public. However, these changes are not good news for privacy, or for competition policy. The critical central control mechanisms, being software, will be easier for Microsoft to change, and harder for its competitors (such as the free software movement) to keep up with. They will also be much more complex and thus more difficult for outsiders to scrutinise for features that threaten privacy, whether deliberately or otherwise.

3. The TCG claims that hardware control is no longer exerted by the TPM. This is again a sophistry. The hardware control is exerted by software in the Nexus and in the applications that run on top of the Nexus. This software generates the hash values that the TPM protects. The TPM is an integral part of the mechanism used to ensure that only authorised hardware and software have access to data protected by TC mechanisms. Without it, the Nexus could be circumvented.

4. The TCG objects to the statement that 'A TPM based platform boots into a known state with a combination of hardware and software that has been 'approved' by the TCPA [TCG]'.

   First, they claim that the platform owner is able to run whatever hardware or software they choose. However, if they run hardware that has not been approved, the TPM will not make available the key material to the Nexus that is required to unseal data, so TC applications won't run (or will run only in a downgraded, low-security mode). This is just as misleading as the claim (see 1 above) that 'you can always turn it off'. If you fit a hardware debugger into your PC, you won't be able to listen to your music if the music is TC-protected.

   Second, they claim that 'The existence of a TPM in a platform does not affect the state to which the platform boots'. This statement is entirely inconsistent with the information so far released publicly about TC. Only if the TPM is satisfied that the hash of the platform configuration is correct will it let the Nexus have access to the stored key material. If the key material provided by the TPM is false, it won't decrypt the OS configuration and other files properly, and the platform will definitely end up in a different state.

   Third, they claim that they will publish protection profiles for hardware vendors to get certification, and that they will run a logo program for approved components, but that they don't impose any obligation on any party to obtain certification. This again is pure sophistry. If the hardware vendor doesn't get his product evaluated to TCG's protection profiles and thus get it approved, then the user's TC software won't work with that hardware.

   In the version 1.0 TCPA, the clear assumption was that TCPA / TCG would maintain lists of approved hardware. In TC's current incarnation it appears that the control function is exercised through application policy servers that will be maintained by application vendors (see also 7 below). As Microsoft writes the most popular applications – Office and Media Player – Microsoft will largely control what hardware and software combinations are permitted in future. This is very much worse than having this control exerted by an industry consortium; it raises exceptionally severe competition policy issues.

   The TCG approval and logo program might mitigate the competitive threat from Microsoft somewhat. Presumably a hardware vendor who obtained TCG certification but whose product was then blocked by Microsoft from being used on any PC on which Media Player was running, would

have a strong case against Microsoft with DG Competition. However, the lack of transparency over hardware approval procedures, and over precisely who will control what, remain a cause of grave concern on both privacy and competition policy grounds.

5. The TCG claims that software attestation must be initiated and authorised by the owner, and remain under the control of the user. This is again a sophistry. The intended use of TC involves frequent software attestation. For example, in DRM applications, the platform will need the TPM to attest to its integrity whenever the user contacts a website to download a song. This leads to a design decision about the dialog between the machine and the user. The TCG seems to imply that in addition to saying something like 'Please confirm that you wish to pay US$1 from your Paypal account to Microsoft Music Services for Bob Dylan's track *Mr Tambourine Man*' there will also be a box saying 'Please give your consent to your TPM attesting the integrity of your Media Player software to Microsoft's server'. I personally find this unlikely. It is much more likely that when taking ownership of a TC PC, the owner will be asked to give general consent to software attestation. If she refuses, that will have the same effect as turning off the TPM – see (1) above.

6. The TCG responds to the TCPA FAQ observation that 'Compatibility between different applications and their data formats can be controlled remotely' by obfuscating the meaning of the word 'control'. The meaning of the FAQ is this: TC enables Microsoft to set up rules on the server that controls Office, and these can have any effect that can be expressed in a rights management language. Microsoft can thus propagate a rule saying, for example, 'No Office file may be exported to Word Perfect', or 'Office file may only be exported to Word Perfect if at some stage they have been modified using a full-price copy of Office Pro, but not if they have been exclusively created and modified using low-cost products such as Microsoft Works'. The only real limits on what they can do are set by the fear of competition lawsuits.

   The TCG response is obscurantist. First, they repeat the essentially meaningless mantra that the platform owner remains in control – where the word 'control' means, in effect, that if you don't like TC you can always go and buy a Mac. They then deny any intention to enable remote control of the platform by any third party – where they are using the phrase 'remote control' in the sense that PC products such as 'pcAnywhere' allow PCs to be remotely controlled by a system administrator. (It is indeed true that such products won't work properly with a TC PC – compare this with TCG's point 4 where they claimed that 'the platform owner is able to run whatever hardware or software they choose on their platform. The fact of the matter is that if you turn TC on, then pcAnywhere won't work properly; you are still free to run it, but for that you have to turn TC off and thus lose access to all your TC-protected content.)

   TCG then goes on to claim that over time TC will 'reduce the exposure of systems to invasive attack by Trojan viruses (sic) and other malicious software'. This is a claim that TC proponents have stopped making at technical conferences as it is simply no longer believed by competent listeners. The fact of the matter is that much malicious software is in fact spyware, and TC will make it much harder for users to block it. In fact, if the EU draft Directive on IP Enforcement passes in its current form, the combination of TC and the Directive will make it illegal for users to defend themselves against such malicious software.

7. In its seventh technical point, TCG claims that they do not propose to run a registration authority for software, but leave that to software vendors. This merely confirms the current industry assumption that it is Microsoft that will control what hardware combinations are admissible (see 4 above). This raises grave competition policy issues. I do not think the Commission should find it acceptable that market entry in the PC peripherals business should be controlled by a company that has been repeatedly convicted of anti-trust offences.

The TCG document ends by making three statements about its goals.

1. TCG claims that DRM is not their goal. But this is not disputed. DRM was the goal of the project initially; now it is ERM (enterprise rights management – that is, protecting things like email rather than just music). This has been publicly admitted by Bill Gates. The economic

analysis indicates strongly that the goal of ERM is to increase the level of lock-in that application users suffer and thus increase the level of software licence fees that can be charged in future for products such as Microsoft Office. (See Ross Anderson, " 'Trusted Computing' and Competition Policy – Issues for Computing Professionals", in Upgrade v 4 no 3, June 2003, pp 35–41; at `http://www.upgrade-cepis.org/issues/2003/3/upgrade-vIV-3.html`.)

2. TCG claims that their governance allows for broad industry adoption. This is untrue. See Professor Koenig's opinion, op. cit.; the minimum membership fee of US$7,500 discriminates against small businesses. The free software community will also suffer serious harm because the TC technology is made available on a paid-licensing basis, rather than zero-cost licensing, as with previous such industry initiatives such as USB and PCI. These issues are elaborated at length by Professor Koenig, who concludes that the TCG violates European competition law on six counts.

3. On the issue of transparency of processing of personal data, TCG expresses the pious hope that 'In no case should any of the platform or component specifications promulgated by TCG lead to a reduced obligation on the part of Data Processors, nor should such specifications make it more difficult for data processors to meet these obligations'. However, TC will make it significantly harder for Member States to enforce data protection law. Application owners can send encrypted upgrades of software that cannot be disassembled or otherwise inspected unless the TC mechanisms are technically broken – an act that the EU is unfortunately about to make illegal. Although in theory a data protection official could send a suspect machine to a laboratory in Canada to be examined, the target of investigation would then complain that any evidence thus obtained was tainted, as the procedure used would have been unlawful if performed in the EU. This would prevent a conviction in some countries.

To sum up, TC presents a real and present threat to the European data protection regime, which has for many years protected European citizens from many of the privacy abuses that are common in the USA. By imposing on Europe a technology developed entirely by US companies and with a view to US conditions, TCG will build into the European infrastructure the very ills that our protection regime was set up to avoid.

TC will make it very hard – and potentially illegal – for data subjects to defend themselves against spyware and other forms of unlawful surveillance. It will greatly strengthen the incentives for software and other vendors to amass personal profile data as a basis for price discrimination. It will introduce into the PC world a unique identifier, and although this can be changed by the user in theory, such identity changes are likely to be cumbersome and expensive in practice. This unique identifier will be used to match data in ways that are not at present economic and that cannot be practically controlled by the data subject. Finally, it will put significant obstacles in the way of agencies seeking to enforce data protection laws in the European member states.

I have already raised the competition policy issues with Cecilio Madero of DG Competition and Jacques Bus of DG Infosoc. DG Internal Market is responsible, inter alia, for privacy policy. In order to mitigate the harm that TC will do to privacy, I urge that the draft EU Directive on IP protection be amended. I will be happy to meet you to discuss how this might be done.

Yours sincerely,

Ross Anderson