SHOULD CONSUMERS TRUST TRUSTED COMPUTING?

Written by George Hariton and
Hasini Palihapitya
Edited by John Lawford
Public Interest Advocacy Centre
1204 – ONE Nicholas St.
Ottawa, Ontario
K1N 7B7

January 2006

With Funding from Industry Canada

The Public Interest Advocacy Centre
(PIAC)
Suite 1204
ONE Nicholas Street
Ottawa, ON
K1N 7B7

Canadian Cataloguing and Publication Data

Hariton, George and
Palihapitiya, Hasini

Should Consumers Trust Trusted Computing?

ISBN 1-895-060-72-9

EXECUTIVE SUMMARY

Security of computer systems and networks is a growing concern in today's society. Although present computer security functions overwhelmingly rely on software, a combination of software and hardware security can theoretically enhance computer security. The Trusted Computing Group (TCG), a consortium of hardware manufacturers, software developers and system integrators, are developing security solutions based on hardware chips and secure software. The hope is that this approach, referred to as Trusted Computing, will provide a higher level of computer security.

Broadly speaking Trusted Computing is a set of features minimizing the damage caused by a successful attacker, through the following initiatives: (1) Memory Curtaining, (2) Secure Input/Output, (3) Sealed Storage, and (4) Remote Attestation.

Trusted Computing has given rise to a number of consumer concerns. The three most pressing of these are:

(1) Enforcement of Digital Rights Management (DRM);

(2) "Locking in" consumers to proprietary software or families of software;

(3) Surveillance of the consumer's activities and other infringements of privacy.

Firstly, Digital Rights Management (DRM) encompasses a number of technological measures that owners of content can take to protect their rights in order to minimize unauthorized copying and distribution. Developer-enforced defenses take two forms: (1) legal rights enforced through the judicial system, based upon the *Copyright Act* and related intellectual property legislation, and (2) through technical protection measures or DRM, a form of content-owner "self-help". Although these DRM anti-piracy measures could help protect the interests of copyright owners, they could also be abused to prevent "fair dealing" uses that are presently legal for consumers.

As Trusted Computing could effectively tilt the balance toward the copyright owner, and away from consumer interests, care must be exercised in preserving the effect of "fair dealing" provisions in the *Copyright Act*. Legislative revisions of the *Copyright Act* should give adequate weight to the ultimate consequences of rigorously limiting how consumers use digital content. Loss of innovation and diminished creativity are two possibilities among numerous undesirable results that consumers may suffer.

The second concern is that Trusted Computing can be used to reduce or block compatibility of software from different sources. A resultant lack of interoperability arising from Trusted Computing would effectively force consumers, once they have started using a particular operating system, to commit to it and continue to purchase upgrades or new applications from the same vendor. Furthermore, it is possible that the "remote attestation" feature of Trusted Computing (which reports to a third party

the status of the user's computer) will increase the pressure on consumers to run certain kinds of software, and may intensify lock-in. This concern is magnified in a market where certain suppliers hold significant market power, as is presently the case in many computer markets.

Trusted Computing also may fall afoul of the *Competition Act*, which regulates "anti-competitive acts", as well as "abuse of dominant position" in a market by a supplier or group of suppliers. These provisions, properly considered with other relevant intellectual property law, may be useful in addressing the possible ills of software lock-in.

The third and final concern related to Trusted Computing are the possible surveillance applications associated with the project, especially those raised by the remote attestation feature. Remote attestation has the potential to limit individual consumer autonomy over their own personal computers. Further, it may allow effortless data mining to occur, as well as enable the creation of detailed user profiles. Significantly, remote attestation could fall under the definition of "transmission data" under the federal government's 'lawful access' proposals contained in Bill C-74, the *Modernization of Investigative Techniques Act* (*MITA*) making computer users' Trusted Computing profiles available to law enforcement with limited judicial oversight.

"Personal information", as defined in the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*), and as interpreted by the Office of the Privacy Commissioner of Canada appears to cover collecting cryptographic certificates through remote attestation. Thus, general design best practices that emphasize privacy, such as positive/opt-in consent provisions related to remote attestation, should be implemented before TC is broadly introduced to the Canadian public.

Current design specifications place the computer user in control of remote attestation. However, refusal to comply may lead to being barred from accessing certain servers and not being able to complete certain transactions. Proposals for Direct Anonymous Attestation, a digital signature scheme that allows anonymous signing, as well as "Owner Override", a feature that would allow a computer owner to generate an attestation that represents any state that the owner wishes to have represented, instead of the actual state of the machine, may protect users' privacy if implemented successfully.

In conclusion, while the proposed infrastructure of Trusted Computing could be useful for enhancing security in the business environment, the benefits to consumers are harder to isolate. Therefore, it is imperative that the TCG play careful attention to addressing consumer needs in terms of DRM, software interoperability, and the privacy issues generated by Trusted Computing, as it becomes ubiquitous in the computing world.

TABLE OF CONTENTS

INTRODUCTION

Computer hardware and software manufacturers presently are investigating ways of improving computer security. Among the initiatives proposed is the "Trusted Computing" (TC) movement. Major vendors Microsoft, IBM, Intel, Sun Microsystems and others have banded together to create the "Trusted Computing Group" (TCG) to investigate security enhancements for computer hardware.[1] Individual software providers are developing independent software solutions for the proposed new hardware platform. While consumers would benefit from increased security, Trusted Computing has given rise to a number of concerns.[2] Three in particular have been raised repeatedly, and merit further consideration:

(1) Will TC expand the capabilities of content providers or owners to restrict the use of their content, under a concept called Digital Rights Management (DRM)?

(2) Will TC be used to deliberately make software applications from different vendors incompatible, and "lock in" users to the products of a particular vendor?

(3) Will TC enable surveillance of users, tracking the programs they use, the content they look at or listen to, and the transactions they engage in?

This paper will describe TC and current plans for its implementation. Next, it will review each of the three concerns mentioned above. The nature of the threat will be discussed and possible consumer safeguards will be described.

Security Issues

Security of computer systems and networks is a growing concern in today's society. Viruses and worms distributed through e-mail attachments and other documents have the potential to do immense harm. Hackers target specific servers and systems, either to obtain confidential information or to inappropriately modify information saved on the server. Denial-of-service attacks bombard a server with messages, creating congestion and impairing normal function.

---

[1] The TCG is a not-for-profit organization formed to develop, define and promote open standards for hardware-enabled trusted computing and security technologies. Additional information can be found on the TCG website, online: https://www.trustedcomputinggroup.org/home/.

[2] These concerns have led Richard Stallman to label this approach "Treacherous Computing", also abbreviated to TC. See Richard Stallman, "Can You Trust Your Computer?" *Free Software Foundation* (October 2002), online: http://www.gnu.org/philosophy/can-you-trust.

Recent studies have shown that typical product software has roughly one security related bug per thousand lines of source code. A typical Unix or Windows system, including major applications, has around 100 million lines of source code, and hence, on average, on the order of a hundred thousand security bugs.[3] The risks caused by these vulnerabilities are aggravated by the increasing number of viruses. According to one website, 32, 982 virus alerts were issued in August of 2005 alone (32, 982 were issued in July of 2005).[4]

Viruses can cause billions of dollars worth of damage. For example, a London-based consulting group, Mi2g, reports that the Blaster virus alone infected more than 300,000 computers in 24 hours and caused $525 million worth of damage.[5]

A number of solutions have been proposed. For example, encryption of information attempts to maintain confidentiality. User authentication screens identify users trying to access a system and thereby attempts to keep out unauthorized persons who might be contemplating some form of malice. Finally, firewalls attempt to keep out viruses and worms.

Unfortunately, attackers are extremely ingenious and, at present, security functions overwhelmingly rely only on software. This leaves PCs and systems vulnerable. A comprehensive defense against security threats requires several approaches. Thus, while all of the defenses discussed in this paper could be implemented by using software alone, a combination of software and hardware will make penetrating these defenses much more difficult.

In recent years, a consortium of hardware manufacturers, software developers, and systems integrators have attempted to develop security solutions based on hardware chips and on software that exploits the security features of the chips. The hope is that this approach, variously called Trusted Computing or Trustworthy Computing (TC), will provide a higher level of security.[6]

---

[3] David Safford, "The Need for TCPA", *IBM Research* (October 2002), online: http://www.research.ibm.com/gsal/tcpa/why_tcpa.pdf. IBM is a major promoter of Trusted Computing and can be expected to highlight security risks that TC aims to combat.

[4] Online: http://www.is.bangor.ac.uk/csoc/virusstatistics.php.

[5] On the other hand, some authors believe that security concerns are overdone. For example, Ross Anderson states, "There is also a growing consensus that security scare-mongering is getting out of hand to the point that the average US business may be spending too much on security rather than too little." Ross Anderson, "Cryptography and Competition Policy – Issues with 'Trusted Computing'", Cambridge University (2003), online: http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tcpa.pdf.

[6] These efforts are consistent with the OECD's recommendation to incorporate security as an essential element of information systems and networks (Recommendation #7). "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security", Recommendation of the OECD Council at its 1037th Session, July 25, 2002, online: http://www.oecd.org/document/42/0,2340,en_2649_33703_15582250_1_1_1_1,00.html.

TRUSTED COMPUTING

The name TC covers a number of security initiatives, including hardware, software, and systems. As previously mentioned, a consortium called the Trusted Computing Group (TCG),[7] was formed in 2003 to develop and support open industry specifications for TC across multiple platform types. Essentially, the TCG intends to promote a standard for a 'more secure' PC.[8] The TCG has developed specifications for the Trusted Platform Module (TPM) used in PCs and other systems, as well as a software interface specification to enable application development for systems using the TPM among other projects.

Without being overly technical, TPMs offer hardware-based security initiatives. They are essentially 'microcontrollers' that store keys, passwords and digital certificates. They are typically contained in the motherboard of PCs, and can potentially be used in any computing device that requires these functions. The nature of the silicon used ensures that the information stored is made more secure from external software attack and physical theft. According to the TCG:[9]

> Security processes, such as digital signature and key exchange, are protected through the secure TCG subsystem. Access to data and secrets in a platform could be denied if the boot sequence is not as expected. Critical applications and capabilities such as secure email, secure web access and local protection of data are thereby made much more secure.

A number of chip manufacturer initiatives, such as LaGrande by Intel,[10] are currently in the works. Currently, Dell, Hewlett-Packard, and IBM have started selling desktop and laptop PCs with TPM chips. Some observers forecast that, by 2010, almost 95 per cent of all computers sold will be equipped with a TPM.[11]

Other hardware initiatives, including a Trusted Server Specification,[12] and a Trusted Network Connect to enable protection of the network, [13] are also in

---

7 Refer to note 1, supra for additional information on the TCG.

8 Online: https://www.trustedcomputinggroup.org/downloads/

9 Trusted Computing Group: Frequently Asked Questions, August 2005, online: http://www.trustedcomputinggroup.org/about/faq/.

10 Mike Ferron-Jones and Luke Girard, "LaGrande Technology & Safer Computing Overview", presentation at Intel Developer Forum, online: http://www.intel.com/technology/security/downloads/LT_overview_fall_idf03.pdf. See also, Intel website, online: http://www.intel.com/technology/security/.

11 Forecast by Roger Kay, vice president of client computing at IDC, reported by CNET *News.Com* (March 16, 2005), online: http://news.com.com/2102-7355_3-5619035.html?tag=st.util.print.

12 Trusted Server Specification (TSS) defines the architecture of a trusted server and how these servers are created, managed and maintained. The specification also provides a blueprint for communication between trusted servers and clients.

13 Trusted Network Connect (TNC) is an open, non-proprietary specification that enables the application and enforcement of security requirements for endpoints connecting to the

development. Meanwhile, other work groups are addressing storage, peripherals, mobile devices and other aspects of the project.[14]

Software initiatives, such as an operating system project by Microsoft, intended to take advantage of the new security features of the TCG specifications, have also surfaced. Microsoft's project has had a checkered history. Originally called Palladium, its name was changed to Next Generation Secure Computing Base (NGSCB). NGSCB was originally scheduled for release as part of Microsoft's next generation operating system, code name Longhorn. However, there are suggestions that NGSCB will be delayed beyond the release of Longhorn, which itself is late.[15] There is no clear timeline for its availability.[16]

The TC movement is chugging ahead, based largely on the hardware components. But, applications tend to be narrowly focused, e.g. protection of encryption "keys". The absence of the wide range of applications promised by the original software thrust is being felt.[17]

---

corporate network. The TNC architecture helps IT organizations enforce corporate configuration requirements and to prevent and detect malware outbreaks, as well as the resulting security breaches and downtime in multi-vendor networks.

[14] As outlined on the Trusted Computing Group website, online: https://www.trustedcomputinggroup.org/about/faq/

[15] Andrew Orlowski, "MS Trusted Computing back to Drawing Board", *The Register*, (May 6, 2004), online: http://www.theregister.com/2004/05/06/microsoft_managed_code_rethink/print.html.

[16] One of the difficulties is that Microsoft seems to have made NGSCB part of its Managed Code initiative. Managed Code has many attractive features, including automatic memory management. This is particularly useful for independent applications developers. Unfortunately, managed code makes the new operating system incompatible with existing applications that will have to be rewritten. In light of fierce opposition from the independent applications developers (on whom Microsoft relies to a great extent to make its operating system attractive to buyers), Microsoft is rethinking its approach. Joel Spolsky, "How Microsoft Lost the API War", *Joel on Software* June 13, 2004, online: http://www.joelonsoftware.com/articles/APIWar.html.

[17] Brian Berger, Executive Vice President at security company Wave Systems, quoted in *CNET News.Com*. Robert Lemos, *News.com* (March 16, 2004), online: http://news.com.com/2102-7355_3-5619035.html?tag=st.util.print.

THE TC PROPOSAL

According to Microsoft's account of trusted computing architecture, the projected innovations are divided, broadly speaking, into four groups, each of which necessitates new hardware to be added to PCs. Although each feature has a different security rationale, they can be used in conjunction with one another:[18]

1. Memory Curtaining

Memory curtaining refers to a strong, hardware-enforced memory isolation feature that prevents programs from being able to read or write one another's memory. Thus, even if an intruder gains access to a PC's memory or control of its operating system, it would still not be able to read or tamper with programs' secure memory. Although this could be achieved purely through software, hardware-based curtained memory increases the difficulty of breaching security. It also simplifies the necessary software and reduces compatibility issues.

2. Secure Input/Output (I/O)

Some intruders collect information on a user by recording what is typed, via a key-logger, or recording what is displayed on a screen, via a screen-scraper. This can capture information such as user ID, passwords, and the contents of e-mails and documents. Secure I/O will provide a secure path from the keyboard to an application, and back from the application to the screen. No other software running on the same PC will be able to determine what the user typed, or how the application responded. Creating secure channels in hardware is simpler and more powerful than creating them in software alone.

3. Sealed Storage

Sealed storage addresses a major PC security failing: the inability of a PC to securely store cryptographic keys. Generally, keys and passwords that protect private documents, accounts and other sensitive information are stored locally on a computer's hard drive, along with the sensitive material itself. Unfortunately this leaves the keys vulnerable to viruses and other intruders.

Instead of storing keys on the hard drive, sealed storage will generate keys whenever they are needed. The generation of these keys will be based in part

---

[18] The following section borrows heavily from the paper on Trusted Computing published by the Electronic Frontier Foundation (EFF). Seth Schoen, "Trusted Computing: Promise and Risk", Electronic Frontier Foundation, online: http://www.eff.org/Infra/trusted_computing/20031001_tc.php **[*Schoen, EFF*]**.

on the identity of the software requesting to use them and in part on the identity of the computer on which that software is running.

If an unauthorized program, or an authorized program that has been modified (e.g. by a virus) tries to decrypt the data, it will fail. Similarly, if the encrypted data is moved to a different machine, attempts at decryption will fail.

Again, sealed storage could be implemented in software alone. However, that would be complicated and processing-intensive. Hardware-based sealed storage is simpler and, therefore, more secure. Hardware-based curtained memory, secure I/O, and sealed memory provides a much higher degree of security to users than is currently available. Even if a virus or other intruder does penetrate a computer's defenses, the damage it can cause will be limited by these measures.

4. Remote Attestation

Remote attestation, broadly speaking, aims to allow 'unauthorized' changes to software to be detected. For example, if an attacker has replaced one of your applications, or a part of your operating system with a maliciously altered version, you would be able to tell that such a change has occurred. Remote attestation is intended to facilitate digital interactions with others, by "reassuring them" about who or what is on the other end of the transaction. It guards against inappropriate access to sensitive or confidential information or systems. It does this by issuing a cryptographic certificate, attesting to the identity of the machine using the certificate, or the identity of the software currently running on the machine. This certificate may, at the PC user's request, be provided to any remote party. The effect is to allow unauthorized changes to software to be detected remotely (i.e. unaltered by a virus). This enables the remote party to avoid sending sensitive data to a compromised system. If your computer should be broken into, other computers can refrain from sending private information to it, at least until it has been fixed.

Remote attestation as originally designed depended on a trusted third party to issue a certificate of attestation to the remote party, and so protect anonymity of the platform user. However, Direct Remote Attestation allows the generation of keys that can be trusted, without revealing the identity of the platform user, and so that can be directly sent to the remote party, without using the services of a trusted third party.[19]

---

[19] "Direct anonymous attestation can be seen as a group signature without the feature that a signature can be opened, i.e., the anonymity is not revocable. Moreover, DAA allows for pseudonyms, i.e. for each signature a user {in agreement with the recipient of the signature} can decide whether or not the signature should be linkable to another signature." Ernie Brickell, Jan Camenisch, and Liquen Chen, "Direct Remote Attestation", February 11, 2004, online: http://eprint.iacr.org/2004/205.pdf.

HARDWARE SPECIFICATIONS: TPM

TCG has published specifications for architecture and a Trusted Platform Module (TPM).[20] As stated above, the TPM is the hardware component of the initiative. It is a microcontroller that stores keys, passwords and digital certificates, and is typically affixed to the motherboard of a PC, but couple potentially be used in any computing device that requires these functions. One of the most significant aspects of TPM design is the nature of the silicon used in its production, which ensures that information stored on the chip is protected from external software attack and physical theft. Furthermore,

> Security processes, such as digital signature and key exchange, are protected through the secure TCG subsystem. Access to data and secrets in a platform could be denied if the boot sequence is not expected. Critical applications and capabilities such as secure email, secure web access and local protection of data are thereby made much more secure. [21]

Desktop, notebook and tablet PCs with TPMs are currently available from Dell, Fujitsu, HP, Intel, Toshiba and others.[22]

The owner of the platform has complete control of the TPM and can turn it on or off at will, reset the chip, assign permissions to software processes external to the chip, and protect the transport of commands exchanged between the chip and remote software. Furthermore, the TPM cannot control what software runs, as it is a 'slave' to higher-level services and applications.

The TPM also assists in implementing protected capabilities and shielded locations (memory, registers, etc), and to protect, store, and report integrity measurements, called Platform Configuration Registers (PCRs).[23] A PCR is an area of memory inside a TPM that is used to store cryptographic hashes.

Finally, the TPM assists in attestation, i.e. vouching for the accuracy of information, using an Attestation Identity Key (AIK), which is created for this purpose. [24] Upon creation, an AIK is tied to a TPM identity, which is then tied to an Endorsement Key (EK). It is thereby possible to prove that the AIK was

---

[20] Online: https://www.trustedcomputinggroup.org/downloads/specifications/. It is referred to by detractors as a "Fritz chip", referring to U.S. senator Fritz Hollings, who sponsored legislation that would have mandated that every PC have anti-piracy measures loaded onto it. The legislation was defeated.

[21] Trusted Computing Group Website, January 3, 2006, online: https://www.trustedcomputinggroup.org/groups/tpm/TPM_FAQ_2005.pdf.

[22] TPMs are currently provided by Atmel, Broadcom, Infineon, Winbond , and others, in discrete and integrated forms. *Ibid.*

[23] TCG Specification, Architecture Overview, Revision 1.2, April 28, 2004, online: https://www.trustedcomputinggroup.org/downloads/TCG_1_0_Architecture_Overview.pdf.

[24] Online: http://trousers.sourceforge.net/faq.html#4.1

created by a genuine TPM without creating a privacy concern. The AIK may be used by a platform's owner to anonymously establish that identity keys were generated in a TPM. This enables confirmation of the quality of the keys without identifying the specific TPM that generated the key. Direct Anonymous Attestation (DAA) is used to conceal the identity of the platform, without having recourse to the services of a trusted third party.

CONSUMER CONCERNS AND REMEDIES

While TC can enhance security, both for users of a platform and for others who interact with them, it also raises a number of interrelated consumer issues. The Electronic Frontier Foundation (EFF) attributes this skepticism and controversy to the impact that TC has in "fundamentally altering trust relationships". The EFF suggests that, "existing designs are fundamentally flawed because they expose the public to new risks of anti-competitive and anti-consumer behavior". [25] These concerns can be broadly grouped into three categories, each of which will be discussed separately with suggested remedies:

(1) Enforcement of Digital Rights Management,

(2) "Locking in" consumers to proprietary software or families of software,

(3) Surveillance of the consumer's activities and other infringements of privacy.

Concern: Digital Rights Management

Digital Rights Management (DRM) encompasses a number of technological measures that owners of content can take to protect their intellectual property and contractual rights. Software developers have long been concerned that their products are too easy to copy without permission and distribute commercially or informally to friends. More recently, with the proliferation of peer-to-peer exchange of music and videos over the Internet, copyright owners have undertaken considerable efforts to protect their property from copying and unauthorized dissemination.

Developer-enforced defenses take two forms: (1) legal rights and their enforcement through the judicial system, and (2) self-help, through technical safeguards.

[25] *Schoen EFF, supra* note 18.

Firstly, copyright or "content" rights, as they are known, are the subject of the *Copyright Act* [26] and related legislation. At the time this paper was drafted, Parliament was in the process of considering major revisions to the *Copyright Act*. Bill C-60, *An Act to amend the Copyright Act*, was introduced in the House of Commons on June 20, 2005.[27] Bill C-60 was primarily designed to address digital issues surrounding copyright by implementing provisions of the 1996 World Intellectual Property Organization (WIPO) Treaties.[28] The primary objectives Bill C-60 included clarifying liability for Internet Service Providers, facilitating the use of the Internet for educational and research purposes, and harmonizing the treatment of photographers with that of other creators. It also included provisions that explicitly addressed hardware components. Specifically, the circumvention of technological protection measures (TPMs) applied to copyright material, and the alteration or removal of rights management information (RMI) embedded in copyrighted material for the purposes of furthering or concealing infringement of copyrighted content would constitute copyright infringement under the proposed amendments.[29] Bill C-60 did not make it past its first reading before Parliament was dissolved for the January 2006 election.

As Canadian copyright legislation is currently in a state of flux, it will not be discussed further in this paper, except for one aspect. There have always been exemptions to the copyright holder's rights that allow users space for "fair dealing".[30] Fair dealing provisions grant individuals a certain amount of leeway to use or reproduce works for private study, research, review, or news reporting that is not considered copyright infringement under the *Copyright Act*.[31] However, by revising copyright laws to place additional limitations and restrictions on these activities, legislators would effectively create monopolies over work. Consumers stand to lose considerably if the balance of incentives to the producer, through monopoly profits, is pitted against the benefits to the public of using copyrighted work for traditional "fair dealing" purposes.

It has been suggested that loss of innovation will arise as a direct result of restrictive digital rights management regimes. As Hal Varian argued regarding trusted computing in the *New York Times*, once innovators have experimented

---

[26] *Copyright Act*, R.S., c. C-30 [***Copyright Act***].

[27] Bill C-60, *An Act to Amend the Copyright Act*, 1st Sess., 38th Parl., 2005 (First Reading, House of Commons, June 20, 2005) **[*Bill C-60*]**.

[28] Bill C-60 proposed to implement the following two treaties: (1) *WIPO Copyright Treaty* (20 December 1996, 36 I.L.M. 65 (entered into force 6 March 2002), and (2) the *WIPO Performances and Phonograms Treaty* (20 December 1996, 36 I.L.M. 76 (entered into force May 20, 2002).

[29] *Bill C-60, supra* note 27, s.34.01, s34.02. See also, "Government of Canada Introduces Bill to Amend the *Copyright Act*", Industry Canada, June 20, 2005, online: http://www.ic.gc.ca/cmb/welcomeic.nsf/261ce500dfcd725985256482006 8dc6d/85256a5d006b9720852570260064a852!OpenDocument.

[30] *Copyright Act*, s.29.

[31] Special provisions in the *Copyright Act* address use of copyrighted material in educational institutions (s.29.4 to s.29.9), as well as in libraries, archives and museums (s.30.1 and following).

and produced a viable idea, they must then approach manufacturers and 'sell', their idea, at which point their bargaining power is reduced.[32] The end result is decreased incentive for user innovation in the first place. Additionally, these restraints may result in decreased competition affecting both technical and content providers, to the ultimate disadvantage of consumers. This diminished competition could have far reaching effects.[33]

Secondly, although anti-piracy measures have long existed, they were software-based, and so were not impenetrable to those with skill. By contrast, TC would be hardware-based, and therefore, more secure. For example, the remote attestation feature could compel PCs to install anti-piracy hardware and software before a copyright owner would allow any of its content to be downloaded. More generally, if a number of servers were to cooperate, a PC would be required to have anti-piracy components in place before any of those servers would interoperate or allow access.

Additionally, TC could make copyright safeguards already built into many CDs and DVDs more effective, which may limit how consumers use these products. For example, Sony BMG recently included surreptitious copyright protection software that buried itself on consumer's Windows-based PCs in about 50 widely distributed contemporary music CDs. [34] The XCP anti-piracy software installed by the Sony CDs, also known as a rootkit,[35] was intended to prevent copying music from CDs to the computer. It installed itself on a user's PC when one of the protected CDs was inserted.[36] The code was virtually indetectable, even to anti-virus software, and served to send information back to the company about frequency of use of the content, among other details. Putting aside the considerable privacy issues that were generated by this practice, Sony BMG's rootkit also exposed users to additional vulnerability to hackers and virus writers

---

[32] Hal R. Varian, "New chips can keep a tight rein on consumers, even after they buy a product", *New York Times* (July 4, 2002), [***Varian***] online: http://www.sims.berkeley.edu/~hal/people/hal/NYTimes/2002-07-04.html.

[33] Ross Anderson has hypothesized, for example, "a small film producer in a minority language might find it even harder than at present to get effective distribution. The effects of this could be both economic and cultural". Ross Anderson, "Cryptography and Competition Policy – Issues with 'Trusted Computing'", Cambridge University 2003, online: http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tcpa.pdf.

[34] Simon Avery, "Sony BMG shoots itself in the foot while firing against music pirates", *GlobeandMail.com* (November 11, 2005), [***Avery***] online: www.theglobeandmail.com/servlet/story/LAC.20051111.IBSONY/BNPrint/Intern.

[35] A "rootkit", so labeled because it installs itself in the root of a PC, is cloaked so it is difficult to find and remove. It is a set of virus-like tools frequently used by hackers to conceal running processes and files from diagnostic and security software. This helps an intruder maintain access to a computer for malicious purposes.

[36] Sony BMG provided a brief warning when customers inserted one of the protected CDs. A 3000-word agreement, which included the following paragraph popped up on screen: "This CD will automatically install a small proprietary software program onto your computer. The software is intended to protect the audio files [on the CD…] and it may also facilitate your use of the digital content". *Avery, supra* note 34.

who could more easily gain control of affected computers.[37] Furthermore, the anti-piracy software itself is alleged to have damaged computers on which it was installed.[38]

This particularly pronounced form of DRM caught the attention of the New York Attorney General, the Department of Homeland Security, and other officials in the U.S.[39] Numerous class action law suits were filed in the U.S., and by January of 2006, poised to settle out of court.[40] However, Sony BMG still faces legal action launched by the Texas Attorney General alleging violations of the state's anti-spyware laws. Two class action suits were also filed in Calgary to ensure that Canadian consumers, who are excluded from the American settlement, remain on equal footing with American consumers.[41]

Additionally, many consumers possess and use unlicensed software, despite DRM initiatives. TC will make it much more difficult to run unlicensed software, as it is obviously a priority to Microsoft and other software vendors to curb such activity. TC further intends to protect application software registration mechanisms so that unlicensed software will be excluded from the new paradigm.[42]

Some commentators advance the possibility that TC would support electronic censorship through these initiatives. Because DRM, in its most extreme form, necessarily implies that only certified programs could be run, and only certified content could be displayed, "at the level of bits, censorship and Digital Rights Management are technologically identical".[43] As explained by Ross Anderson:

> [D]igital objects created using TC systems remain under the control of their creator, rather than under the control of the person who

---

[37] Sony BMG issued a patch that users could download from Sony's site; however, this update was also riddled with problems.

[38] Gil Kaufman, "Sony BMG Faces Lawsuits in Canada Over Anti-Piracy Software", *MTV.com* (January 6, 2006), online: http://www.mtv.com/news/articles/1519871/20060106/index.jhtml?headlines=true.

[39] Arik Hesseldahl, "Spitzer Gets on Sony BMG's Case", *BusinessWeek Online* (November 29, 2005), online: http://businessweek.com/print/technology/content/nov2005/tc20051128_573560.htm.

[40] The settlement seeks to compensate consumers for harm they suffered from the Sony CDs and places limits on Sony's future use of TPMs (See note 52). It compensates most purchasers with a copy protection free replacement CD as well as the choice of either $7.50 U.S. plus one free album download or three free album downloads. Michael Geist, "Rootkit Fiasco Shows Sterner Laws Needed", *Toronto Star* (January 2, 2006), online: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1136155809237&call_pageid=968350072197&col=969048863851.

[41] Over 120,000 affected CDs were sold in Canada. Gil Kaufman, "Sony BMG Faces Lawsuits in Canada Over Anti-Piracy Software", *MTV.com* (January 6, 2006), online: http://www.mtv.com/news/articles/1519871/20060106/index.jhtml?headlines=true.

[42] Ross Anderson, " 'Trusted Computing' Frequently Asked Questions", August 2003, [***Anderson, FAQ***] online: http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html.

[43] *Varian, supra* note 32.

> owns the machine on which they happen to be stored […] Given such possibilities, we can expect TC to be used to suppress everything from pornography to writings that criticize political leaders. [44]

Certainly, other less severe applications also exist for electronic censorship. For example, TC could facilitate the design of applications that could potentially delete pirated music under remote control. Thus, a TC-compliant media player could detect electronic watermarks and then react accordingly. Regardless of the copyright issues motivating this theoretical use, it should remain a priority to safeguard consumer autonomy and privacy.

Remedy: Digital Rights Management

The principal consumer remedy for overreaching DRM is contained in "fair dealing" provisions of the *Copyright Act*.[45] Although there is room for disagreement over the extent of fair dealing that should be allowed, legislative revisions should give adequate weight to the ultimate consequences of rigorously limiting how private citizens use copyrighted material.

If we use Bill C-60 as an example of how legislators intend to incorporate elements of TC with copyright laws, then it is clear that the line between legislative and technical safeguards will be blurred. Recall, Bill C-60 was introduced as a means of incorporating international treaty obligations into domestic legislation. As the amendments did not take force, these treaty obligations still have not been honored. Thus, future amendments to the *Copyright Act* will likely resemble Bill C-60 in terms of compliance with WIPO obligations. Specifically, the *Copyright Act* would be broadened by the legislation to limit the circumvention of technological protection measures (TPMs) and the alteration or removal of rights management information (RMI) embedded in copyrighted material.[46]

Fair dealing provisions of the *Copyright Act* presently permit users, for example, to copy musical sound recordings (to certain recording media, but not "devices") for private, non-commercial use.[47] These rights were preserved under the proposed amendments. However, if manufacturers employ technical DRM strategies, then consumers' fair dealings rights will be unduly restricted. Thus, "it could be possible for the rights holder of a musical sound recording to place technological protection measures on that recording to prevent this otherwise

---

44 *Anderson FAQ, supra.* note 42.

45 *Copyright Act*, s.29.

46 See note 28 *supra*.

47 *Canadian Private Copying Collective* v. *Canadian Storage Media Alliance* [2005] 2 F.C. 654 (C.A.).

legal and legitimate use of the material."[48] Such limitations could be particularly problematic in light of experiences such as the Sony BMG rootkit case discussed above.

As a corollary to this argument, critics have argued that technological restrictions reinforced by legislation stand to legitimize breaches of privacy. Greg Hagen, for example, has argued of the Sony BMG rootkit debacle, the "fact that the spyware was embedded in XCP should give pause to those who support Bill C-60, which lends legitimacy to technological measures (to protect copyright) that embed spyware."[49] Further, outspoken privacy promoter, Ian Kerr, has argued that statutory silence about the permissible scope of the use for TPMs poses a significant threat to privacy.[50] He contends:

> Any law protecting the surveillance technologies used to enforce copyright must also contain express provisions and penalties that protect citizens from organizations using those TPMs to engage in excessive monitoring or the piracy of personal information.[51]

Therefore, legislative revisions, such as those proposed by Bill C-60, should carefully consider these practical contradictions. As TC-enhanced DRM measures stand to give content owners and applications suppliers more detailed control over their intellectual property, restrictive legislative amendments may serve to strengthen manufacturers' control at the expense of users' legal rights.

Professor Michael Geist, Canada Research Chair in Internet and E-Commerce Law at the University of Ottawa, suggests that the provisional settlement of class action proceedings reached by Sony BMG provides the starting point for a future

---

[48] Bill C-60: An Act to Amend the *Copyright Act*, Legislative Summary, 20 September 2005, at pp. 21, online: http://www.parl.gc.ca/common/Bills_ls.asp?lang=E&Parl=38&Ses=1&ls=C60&source=Bills_House_Government#Background.

[49] Greg Hagen, "Circumventing Privacy: When Technological Measures Become Spyware", December 06, 2005, online: http://www.anonequity.org/weblog/archives/000248.php.

[50] Ian R. Kerr, "If Left to Their Own Devices: How DRM and Anti-circumvention Laws Can Be Used to Hack Privacy", in *In the Public Interest: The Future of Canadian Copyright Law*, (Toronto: Irwin Law, 2005) 167 at 170, online: http://idtrail.org/content/view/173/42/.

[51] Ian Kerr presents the following three recommendations to integrate protection of personal privacy with copyright infringement measures to be contained in an "anti-circumvention" provision:

1. An express provision prohibiting the circumvention of privacy by TPM/DRM, notwithstanding license provisions to the contrary.
2. An express provision stipulating that a DRM license is voidable when it violates privacy law.
3. An express provision permitting the circumvention of TPM/DRM for personal information protection purposes.

Ian R. Kerr, *Ibid.*

Digital Rights Management Protection Act (DRMPA).[52] He notes that our future "DRMPA must include consumer protections, privacy protections, security protections, interoperability, and appropriate oversight". Furthermore, he argues that such legislation is necessary to protect consumers from impenetrable DRM schemes. He advises, "Rather than pushing for protection for DRMs, it is apparent that we need protection from DRMs and DRMPA would be a smart step in that direction".[53] Obviously, any action taken in this direction would have to be coordinated with those taken in terms of amending the *Copyright Act*.

Finally, controlling DRM activity is not just a copyright and fair dealings issue. Because aggressive DRM tactics can cloak significant anti-competitive behaviour, the Competition Bureau should scrutinize DRM safeguards and activity carefully to monitor and prevent abuse of dominance activities. While purchasing power might normally curb some of the negative DRM activities conducted by software manufacturers, this approach is inadequate in the present case. Ultimately, consumers will be left with limited choice in the marketplace if DRM practices are not properly regulated by legislation.

Concern: 'Locking In' Consumers

The second concern, that software manufacturers could exploit Trusted Computing to disrupt the interoperability of software, is related to the first issue of Digital Rights Management enforcement. Software 'lock-in' occurs as a result of a lack of interoperability between software products. It would effectively force consumers, once they have started using a particular operating system or application, to continue using it and to purchase upgrades etc. from the same

---

[52] Sony BMG has agreed to the following 10 limitations on the use of copy-protection software until 2008:

1. No further use of XCP or Media Max
2. Ensure that the DRM will not be installed on users' computers until the user accepts the end-user license agreement.
3. Ensure that an uninstaller for the copy-protection software is made readily available to consumers.
4. Fully disclose any updates to the copy-protection software.
5. Ensure that the EULA accurately discloses the nature and function of the software in plain English
6. Obtain comments about the EULA from an independent oversight person.
7. Obtain an expert opinion that the copy-protection software does not create security vulnerabilities.
8. Only collect limited personal information necessary to provide enhanced CD functionality.
9. Include full disclosures of the copy-protection software on the CD jewel case.
10. Fix any software vulnerabilities that may arise from the copy-protection software.

This list is taken from Geist's summary of the settlement. "The Start of a DRM Protection Act", Michael Geist, December 29, 2005, online: http://www.michaelgeist.ca/index.php?%20option=com_content&task=view&id=1052.

The provisional settlement reach in New York State can also be accessed online: http://www.sunbelt-software.com/ihs/alex/sonysettleme23423423434nt.pdf.

[53] Geist, *Ibid*.

vendor, to the extent these products are intended to work together. Software lock-in would limit choice in the marketplace and competition among software developers.

To borrow Ross Anderson's example, TC would dramatically increase the costs of switching away from Microsoft products (like Office) to rival products (e.g. OpenOffice). While switching software in a work setting is relatively easy to implement at present, switching software may become a burdensome project once TC is widely implemented. Using a law firm context in his example, Anderson explains:

> In five years' time, once [the law firm has] received TC-protected documents from perhaps a thousand different clients, they would have to get permission (in the form of signed digital certificates) from each of these clients in order to migrate their files to a new platform. The law firm won't in practice want to do this, so they will be much more tightly locked in, which will enable Microsoft to hike its prices.[54]

Thus, lock-in pressures arise not just from compatibility within a user's operations. As the example above illustrates, since documents are frequently traded as e-mail attachments, users must have compatible word processing software in order for such exchanges to succeed. These externalities intensify lock-in pressures.[55]

TC has the potential to exacerbate lock-in pressures through introduction of hardware security measures. Proprietary systems exist today, of course. But they are implemented in software, and it is usually possible to reverse engineer and build emulators (so that different-source software can operate in a mode that allows interoperability). While in-depth analysis of technical details is beyond the scope of this paper, features of Trusted Computing could significantly hinder such emulation. Curtained memory could make emulation much more difficult because this feature prevents programs from being able to read or write one another's memory. Further, sealed storage could require authorization, through keys, to interoperate with any given software, and the keys may be withheld from the user.[56]

However, remote attestation is the most pressing concern leading to software lock-in. Specifically, remote attestation will increase the pressure to run certain

---

[54] *Anderson FAQ, supra* note 42.

[55] Ross Anderson theorizes about Microsoft's profit driven motivations for engaging in TC. He explains, citing the opinions of software economists, that an incumbent in a maturing market, such as Microsoft with its Office product, can grow faster than the market only if it can find ways to lock in its customers more tightly. TC can be made profitable by such efforts. Ross Anderson, *Ibid*.

[56] As mentioned above, current specifications for the TPM chip provide for full control by the platform user.

kinds of software.[57] For example, servers might refuse to complete transactions unless the client is running specified software. Even though remote attestation isn't currently being implemented, lock-in pressures attributable to *remote transactions* exist today. The most common example is web sites that can be accessed only through Microsoft's Internet Explorer browser.

The introduction of remote attestation has the potential to magnify such effects. The most urgent concern arising from implementation of remote attestation certainly rests in software developers' theoretical ability to periodically check that original versions of software remain unaltered. They could also, in theory, check that unlicensed versions of software are not installed. This objective would be achieved through certificates of attestation, which would identify the specific machine and the software on it. The Electronic Freedom Foundation (EFF) points to remote attestation's rigid design features that will allow an owner to completely disable attestation, but will not allow her to make an attestation that does not accurately reflect the current state of her PC.[58] As the EFF points out, this approach benefits the computer owner only when the remote party to whom the attestation is given has the same interests as the owner. Thus,

> If you give an attestation to a service provider who wants to help you detect unauthorized modifications to your computer, attestation benefits you. [However,] if you're required to give an attestation to someone who aims to forbid you from using the software of your choice, attestation harms you.[59]

Users would have the option not to provide remote attestation. However, refusing to comply, according to the Electronic Freedom Foundation (EFF), would be difficult. As the EFF explains:

> [A]ttestation can be used to create barriers to interoperability and access, so users will face an enormous amount of pressure to present an attestation. It's economically unreasonable to assume that a technology will benefit people solely because they can decide whether to use it. [60]

Thus, access and interoperability could be refused to machines with "inappropriate" or "unauthorized" software, including, perhaps, software from competing suppliers. In fact, lock-in is much more of a worry in a market where one supplier has dominant market power. The fear is that Microsoft, for example, will be able to leverage its existing market leadership even farther, ensuring that

---

57 *Anderson FAQ, supra* note 42; Lucky Green, "Trusted Computing Platform Alliance: The Mother(board) of all Big Brothers", *Cypherpunks.to*, online: http://www.cypherpunks.to/TCPA_DEFCON_10.pdf; *Schoen EFF, supra* note 18.

58 *Schoen EFF, supra* note 18

59 *Ibid.*at pp.11.

60 *Ibid.*

its products will not interoperate with others, thereby creating an unbalanced software market.

Remedy: 'Locking In' Consumers

The role of TC in facilitating lock-in must be examined in the wider context of the tension between open systems, on the one hand, and proprietary systems, on the other. [61] Proprietary systems are not objectionable per se. For example, Apple has long deliberately kept its system as closed as possible. The merits of such an approach are subject to much debate. Negative aspects include the dearth of applications and the higher prices charged in the face of weak competitive forces. Positive aspects include a better control of system performance, and much higher security against viruses and other attackers, which don't have the multiple points of entry of an open system.[62]

Usually the market, reflecting customer preferences, sorts out the desirability of open versus proprietary systems. Indeed, Apple's small market share suggests that customers generally prefer open systems and wide-ranging interoperability. However, market forces may not always be sufficient to ensure that consumers' preferences are adequately reflected. If market power is abused by a firm or firms, possible solutions may be generated through the proper legal framework.

To this end, the *Competition Act* [63] purports to promote efficiency within the Canadian economy and is intended to provide consumers with competitive prices and product choices.[64] Part VIII of the *Competition Act* provides an avenue through which the Competition Tribunal can adjudicate anti-competitive behaviour. The Tribunal has statutory authority to make a number of remedial orders where it finds reviewable practices, and is also sanctioned to permit private rights of action in certain cases as well.

"Anti-competitive acts" are defined in s.78(1)(g) of the *Competition Act*, as including "adoption of product specifications that are incompatible with products produced by any other person", which directly relates to the issue of software lock-in. Further, the "Abuse of Dominant Position" provisions contained in s.79 of

---

[61] The term "open source" indicates that the source code is available to the public. "Proprietary software" on the other hand, is software that is owned by a single organization or individual.

[62] There is a trade-off between open systems and security, even if the trade-off is weak. Open interfaces allow attackers the toe-hold they need to access the targeted system. The more "closed" the system, the more secure it seems to be. Thus, Apple is widely recognized for the production of systems that are reasonably closed, quite secure, relative to Microsoft. In turn, Linux and Linux-based applications are the most open, and may be most vulnerable to security risks.

[63] *Competition Act*, R.S., 1985, c-34, [***Competition Act***].

[64] See generally, George S. Takach, "B. Competition Law", Chapter 5, Commercial Law, *Computer Law*, 2nd ed. (2003) (QL) [***Takach***].

the *Competition Act* provide that where an entity substantially controls a class of business, and that entity engages in anticompetitive acts that are likely to prevent or lessen competition substantially, the Competition Tribunal may prohibit the behaviour in question. However, subsection 79(5) of the *Competition Act* provides that any act engaged in pursuant only to the exercise of any right under the *Copyright Act*, the *Patent Act*,[65] and the other intellectual property statues is not an anticompetitive act.

As George S. Takach explains, intellectual property legislation and the *Competition Act* offer seemingly contradictory approaches to problems like software lock-in. He writes:

> the intellectual property regimes […] provide more or less extensive monopoly rights to holders of intellectual properties, and the *Competition Act* […] attempts to curb perceived and potential abuses of such intellectual property rights. [66]

A thorough discussion of the nuanced interaction of these legislative provisions is beyond the scope of this paper. However, it is abundantly clear that TC is a tool that could easily run afoul of Canadian competition law by intensifying or even facilitating software lock-in. Thus, the law must address the concerns related to software lock-in, in order to properly protect consumer interests.

Finally, as mentioned above TC could, in principle, be used to stop platform owners from modifying or tinkering with software on their platform. However, TCG has committed repeatedly to give users complete control over the security measures in TC and in the TPM chip. In particular, the platform owner will be able to disable the TPM, either selectively or completely.[67]

But, choosing to turn the TPM chip off is not the same as refusing to participate in the attestation scheme espoused by TC. As stated above, refusing to provide attestations is not a realistic solution, according to the EFF. Rather, the EFF advocates a solution it calls Owner Override. This feature would allow a computer owner to generate an attestation that represents any state that the owner wishes to have represented, instead of the actual state of the machine. As the EFF explains:

> [a] user centered, pro-competitive approach to attestation features would give the owner the power to guarantee that attestation is never abused for a purpose of which the owner disapproves,

---

65 *Patent Act*, R.S., c.P-4.

66 He further notes that Canada is not alone in this contradiction, with the EU facing a similar struggle. *Takach, supra* note 64, at pp. 6.

67 The concern is lock-in of software: operating systems and applications. Given the adoption of open standards by TCG, hardware lock-in is much less of a problem, and has largely been resolved by users insisting on compatibility.

> maximizing computer owners' practical control over their computers in real-world network environments.[68]

Owner Override features would remove the toolbox that allows the trusted computing architecture to be abused for anti-interoperability and anti-competitive purposes without undermining TCG architecture.[69] Thus, incorporating the Owner Override feature would add flexibility benefiting consumers.

Such an 'anonymization' scheme should be studied in Canada in light of the *Competition Act* and Canadian privacy law before it is adopted or sanctioned by Canadian policymakers. However, such an idea has the advantage of returning some measure of control to users in the restrictive TC environment.

Concern: Surveillance and Privacy

The third and final concern related to Trusted Computing is the possible surveillance applications associated with the project, especially those raised by the remote attestation feature. The privacy implications associated with TC are often ignored, but should be seriously considered as the "personal computer sovereignty" of consumers is at issue.

As described above, remote attestation aims to allow "unauthorized" changes to software to be detected. As originally designed, remote attestation required a computer owner to allow a third party to verify the hardware and software on his or her machine. If these were "authorized", and not modified, the "trusted third party" would issue a certificate of attestation. The computer owner could then proffer this certificate to servers and other users on the network. This would assure the latter that interacting with the computer owner's machine would not pose certain well-defined security threats, and that any content downloaded would be properly safeguarded.

While in theory remote attestation has the potential to greatly increase computer security, critics caution, "buyer beware". Remote attestation also has the potential to limit individual autonomy with respect to PCs. For example, the EFF has commented:

> TCG attestation conspicuously fails to distinguish between applications that protect computer owners against attack and applications that protect a computer against its owner. In effect, the computer's owner is sometimes treated as just another attacker or

---

[68] *Schoen EFF, supra* note 18 at pp.11.

[69] For a comprehensive review of integrating remote attestation with Owner Override features, consult *Schoen EFF, supra* note 18 at pp. 13 and following.

> adversary who must be prevented from breaking in and altering the computer's software.[70]

Thus, the computer owner is forced to relinquish sovereignty over her computer.

Among the numerous possible negative effects that will burden consumers, compromised privacy is of particular concern. Remote attestation has the potential to allow effortless data mining to occur. A trusted third party can, in theory, collect a substantial amount of information on the contents of a user's computer, and also monitor the user's activity to some degree by linking requests for authentication certificates. Even if the user remains anonymous, compiling such details can be used to develop user profiles. Further, if the trusted third party colludes with some of the companies to whom certificates of attestation are destined, this information can also be used to determine the true identity of the user.[71]

Another issue not considered by the TCG is that TC remote attestation certificates and other features of TC also are likely to be considered "transmission data" under the federal government's recent 'lawful access' proposals. Those proposals recently have culminated in Bill C-74, the *Modernization of Investigative Techniques Act* (MITA), [72] that died on the Order Paper but is likely to be re-introduced in the next Parliament. The definition of "transmission data" from *MITA* reads:

> "transmission data" means data relating to the telecommunications functions of dialling, routing, addressing or signalling that identifies or purports to identify the origin, type, direction, date, time, duration, size, destination or termination of a telecommunication generated or received by means of a telecommunications facility or the type of telecommunications service used and includes any information that may be obtained under subsection 492.2(1) of the *Criminal Code*.

A thorough analysis of whether the remote attestation features of TC satisfy this definition is beyond the scope of this paper. However, it is plausible that TC remote attestation information (computer type, operating system and possibly location or IP address, etc.) would be covered by *MITA* and therefore would have to be produced to the government by certificate or other TC players. *MITA* and the lawful access proposals that proceeded it have been heavily criticized by consumer and civil liberties groups for being overbroad, lacking in judicial

---

[70] *Schoen, EFF supra* note 18 at pp 5.

[71] William Arbaugh, "The TCPA; What's Wrong; What's right and what to do about it", July 20, 2002, online: http://www.cs.umd.edu/~waa/TCPA/TCPA-goodnbad.pdf.

[72] Bill C-74, *An Act regulating telecommunications facilities to facilitate the lawful interception of information transmitted by means of those facilities and respecting the provision of telecommunications subscriber information,* 1st Sess., 38th Parl., 2005 (Short Title: *Modernization of Investigative Techniques Act*).

oversight and reporting mechanisms.[73] In particular, they are criticized for a lower standard of proof, and reduced judicial oversight, required of authorities before obtaining information.

The question that arises with TC, therefore, is whether we wish to create yet another data stream that the government is authorized to effectively wiretap with minimal oversight. This potential for increased government surveillance of personal computing architecture should be noted by the TCG and addressed in the standards, as well as studied by lawmakers and policymakers in the context both of TC and acts such as the *MITA*.

Remedy: Surveillance and Privacy

The idea of the ability to control one's own computer and be shielded from electronic espionage is a new right, but one based on a set of fundamental freedoms we all presently enjoy. Protecting informational privacy, for example, is a widely accepted right as it is imperative that individuals maintain control over the collection, use and disclosure of their personal information. To this end, legislation has been enacted to limit the collection and use of such data. Tying this informational privacy right to a nascent "computer autonomy" right seems sensible (or at least plausible) in light of the level of control of TC over end users and its potential to collect personal information. However, in order to use the personal information law of Canada to build this new consumer counter-right to TC architecture, the preliminary hurdle of showing TC information is "personal information" must be cleared.

"Personal information" is defined in s.2 of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*),[74] and includes information that can be used to identify individuals, such as: names, addresses, telephone numbers, dates of birth, race, and family status.[75] Personal information is often contained on individual PCs in a number of different ways, too varied and complicated to discuss in this paper. However, two aspects of personal computing, web browsing history, and electronic passwords, are of particular concern.

A case was brought before the Office of the Privacy Commissioner of Canada in which a broadcaster was accused of collecting personal information via a Web

---

[73] See, for example, the "lawful access" information pages on the website of the Canadian Internet Policy and Public Interest Clinic (CIPPIC) at http://www.cippic.ca/en/projects-cases/lawful-access/.

[74] *Personal Information Protection and Electronic Documents Act* 2000 c.5, [***PIPEDA***].

[75] See generally, Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario, "Privacy and Digital Rights Management (DRM): An Oxymoron?" October 2002, online: http://www.ipc.on.ca/docs/drm.pdf [***Cavoukian, DRM***].

site.[76] In this case, the complainant's firewall software notified him of a security threat every time he tried to access a certain website. The broadcaster's advertising server tried to access to the complainant's NETBIOS information before allowing him to access the website. A NETBIOS is a computer's common or "friendly" name related to its Internet Protocol (IP) address,[77] which if traced, could lead to information such as recently visited web sites or passwords. Principle 4.3, Schedule 1, *PIPEDA* requires that the knowledge and consent of an individual are required for the collection, use, or disclosure of personal information, except where inappropriate.[78] The Commissioner was satisfied that in some circumstances, and this case in particular, a NETBIOS might be used to obtain information traceable to an identifiable individual. He determined, therefore, that a computer's NETBIOS was personal information for the purposes of *PIPEDA*.

Although a thorough technical analysis of remote attestation is beyond the scope of this paper, the privacy issues it raises are similar to those of the case discussed above. If harvesting NETBIOS information is problematic because it can be traced back to personal information, then by analogy, collecting cryptographic certificates may also lead to similar privacy issues.

As remote attestation is still being designed and technical specifications refined, there is no guarantee that remote attestation will not lend itself to such abuses. The Office of the Privacy Commissioner of Ontario has issued guidelines for designing privacy into technology. The "7 Essential Steps for Designing Privacy into Technology", include: defining the privacy expectations of the public and conforming with legislative requirements; assessing human and informational resources with a focus on personally identifiable data (collection, processing etc.); and deployment of methodology for privacy risk management at the systems level, and introduction of these rules and controls at the source code level.[79]

---

[76] *PIPED Act* Case Summary #25, "A broadcaster accused of collecting personal information via Web site", November 20, 2001, online: http://www.privcom.gc.ca/cf-dc/2001/cf-dc_011120_e.asp.

[77] NETBIOS is an acronym for Network Basic Input Output System. It is an Application Program Interface (API) that augments the DOS BIOS by adding special functions for local area networks (LANs). Almost all Windows-based LANs for PCs are based on NETBIOs.

[78] For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information.

[79] The 7 Essential Steps for Designing Privacy into Technology:

1. Define privacy expectations of the public and identify legislated requirements
2. Develop privacy policies and principles
3. Undertake an assessment of human and informational resources with a focus on personally identifiable data (collection, processing, management, flows and storage).
4. Undertake a threat risk assessment by completing a Privacy Impact Assessment
5. Deploy methodology for privacy risk management at the systems level
6. Introduce the rules and controls developed in the previous step at the source code level

By way of illustration, general design best practices flowing directly from the consent principle under *PIPEDA* would include use of positive/opt-in (express) consent provisions.[80] In compliance with Principle 4.3.6, express consent should be obtained when the information is likely to be considered sensitive. Further, the organization gaining access to personal information cannot assume individual consent unless it is expressly provided. Thus, consent could be obtained by using a pop-up box, for example, that informs individuals about the information being collected, what it will be used for, and so on. However, the default choice for the user should be an "opt-in" set-up choice for remote attestation and other privacy-invasive TC features; that is, the radio button should be set to 'off' by default. Other principles of *PIPEDA* should be implemented in TCG design in a similar fashion.[81] It would be advisable for the TCG to consider these issues, and the potential legal ramifications of overlooking them, while there is still time to implement privacy safeguards related to TC in general and remote attestation in particular.

The current TCG specifications place the computer user in control of remote attestation. Specifically, the user can choose whether to enable or disable remote attestation, or allow it to operate selectively. This allows the user to avoid the risks mentioned above. However, as previously mentioned, because the average PC user lacks knowledge about design specifications or the privacy risks related to remote attestation, the potential for abuse is great, unless significant efforts to educate users are undertaken by the TCG.

As discussed previously in the DRM section, some commentators believe that users will be under significant pressure to comply with remote attestation. Refusal to comply may lead to being barred from accessing certain servers and not being able to complete certain transactions. Thus, for customers to make informed choices about whether or not to provide remote attestation, there must be explicit disclosure about the consequences of participation. Machines capable of providing remote attestation should be required to include a simplified description of the process, that includes the consequences to the owner of the machine, and obtain user consent.

Finally, TCG's current specifications provide for Direct Anonymous Attestation (DAA), a protocol that could protect users' privacy. DAA is a digital signature scheme that allows anonymous signing. Verifiers would be permitted to confirm that an authorized party signed a message, without revealing the identity of the specific signer. Further, the trusted third party requirement would be waived.

---

7. Deploy and audit, through a model of continuous improvement. Review expectations and requirements.

Online: www.ipc.on.ca/userfiles/page_attachments/7steps.pdf.

[80] "Office of the Privacy Commissioner of Canada, "Fact Sheet: Determining the appropriate form of consent under the Personal Information Protection and Electronic Documents Act", online: http://www.privcom.gc.ca/fs-fi/02_05_d_24_e.asp.

[81] See generally, *Cavoukian, DRM, supra* note 75.

Instead, the TPM would generate a non-user-unique key that would be accepted as suitable authentication if it falls within a group signature. A user would be permitted to vary such keys from authentication to authentication, making it difficult for a remote party to build a profile.

If Direct Anonymous Authentication can be implemented successfully, many privacy concerns described above would be alleviated. For example, if a user talks to the same verifier twice, the verifier would not able to determine whether or not communication is with the same user as before or with a different one. This may go some way towards restricting data profiling and address the issue of complete opt-in or opt-out of TC features such as remote attestation. In sum, however, it is fair to say that there is a range of privacy issues that have not been fully explored with trusted computing.

Conclusion

While TC offers promising solutions towards building a culture of information security, it is not without its downside. The potential benefits of TC should be assessed in the different environments in which it will be used. While the proposed infrastructure could be useful for enhancing security in the business environment, especially in corporate networks, the benefits to consumers are harder to isolate. While TC offers some improvements in terms of protected storage and the opportunity to use digital pseudonyms for transactions, TC may disadvantage consumers, through pronounced enforcement of DRM, privacy invasions under the guise of remote attestation and anti-competitive "lock-in" of consumers to one operating system or set of applications. [82]

Therefore, it would be advisable to conduct additional study of Trusted Computing on the following topics. First, how should legislative revisions to the *Copyright Act*, such as those proposed by Bill C-60, be coordinated with the possible introduction of a Digital Rights Management Protection Act? Second, to what extent will the design specifications of TC, especially the remote attestation feature, comply with the *Competition Act* and other relevant intellectual property legislation? As TC continues to gain momentum, and TPM chips begin to find their way into consumers' lives, it is necessary to ensure that legislation keeps pace with technological advancement.

Additionally, even at this nascent stage in TC, consumers must have access to all the necessary information in order to make informed decisions. Software licenses are complicated and difficult for the layperson to understand. As a

---

[82] "Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG group)", Adopted on January 23, 2004 by the Article 29 Data Protection Working Party, 11816/03/EN, online: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp86_en.pdf.

result, often consumer consent is not informed consent, and does not reflect a true choice. Therefore, it is important that content providers make explicit and clear disclosure of any limitations on the use of their products. In addition to the usual licenses, it would be desirable to produce a document that explains to consumers in a simplified manner any technological limitations that will affect their use of the product. Any unusual provisions should be highlighted. Finally, it is also important that any revision, and tightening of these limitations not be effective retroactively.

In conclusion, as the use of TPMs may well become ubiquitous, it is imperative that the TCG pay careful attention to addressing consumer needs in terms of DRM, software interoperability, as well as surveillance and privacy issues generated by TC. The potential benefits must be weighed against negative consequences that consumers may disproportionately suffer, and a balanced and fair strategy should be employed, or legislation of TC may be required.