International Working Group
on Data Protection
in Telecommunications

675.33.17 6 September 2006

Working Paper

Trusted Computing, Associated Digital Rights Management Technologies, and Privacy: Some issues for governments and software developers

40th meeting, 5-6 September 2006, Berlin

Trusted computing and associated digital rights management technologies (TC/DRM) can bring many benefits for privacy. Improved security of the systems within which personal information is collected, accessed, used, and disclosed is a laudable goal. However, informed responsible implementation of these complex technologies is required in order to avoid unintended risks to personal privacy.[1]

Privacy risks centre on the remote attestation feature but include the potential for long-term lack of control over an organisation's documents. For example, one concern that has been identified is the possible compromise of an individual's right to access personal information held by an agency if the rights to a document containing that personal information have expired.

There can be special issues for governments implementing TC/DRM technologies because of their responsibilities under legislation mandating archiving requirements. For this reason, the recommendations that follow are largely but not exclusively targeted to government agencies. Private sector organisations will in most cases have similar, if not legislated, responsibilities.

Recommendations

The Working Group recommends that governments consider the potential hazards to privacy and the long-term maintenance of official government records that may result from ill-considered implementation of these technologies. Collaboration with other governments in engaging with the vendor community may be the most effective way of responding to those potential hazards.

Governments should establish policies to ensure that the benefits of implementing TC/DRM technologies in relation to government records are not outweighed by unintended privacy-invasive effects.

Governments should consider adoption or adaptation of the principles and policies developed by New Zealand[2] and summarised here as:

[1] See also IWGDPT, *Common Position on Privacy and Digital Rights Management*, adopted 4/5 May 2000 < http://www.datenschutz-berlin.de/attachments/234/co_en.pdf>

[2] New Zealand State Services Commission, *Trusted Computing and Digital Rights Management Principles and Policies*, version 1.0, 25 September 2006.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

Governments should not implement TC/DRM technologies in ways that may

1. compromise subject access rights, or
2. endanger the confidentiality and integrity of official records, or
3. endanger the privacy of personal information, or
4. compromise the security of government information systems.

The Working Group recommends and encourages software developers and suppliers of TC/DRM products to make themselves aware of the challenges that governments may face in the adoption and implementation of trusted computing and digital rights management technologies. Some of these issues may differ from those faced by business users of TC/DRM, while many will be the same. Suppliers should ensure that they are able to accommodate government requirements for transparency of operation of these systems and applications.

Suppliers may often find that governments will need full knowledge of and consent to:

1. external encumbrances on records,
2. data flows, especially those involving the collection of personal information,
3. communications outside government systems (including attestation and other background communications),
4. regimes that control and permit access to government-held information, and
5. data safety concerns around harmful content such as viruses and any other security implications.

Suppliers should be prepared to provide governments with independent verification that their systems operate as their communications specifications describe.