



Privacy Commissioner  
Te Mana Matapono Matatapu

## DIGITAL RIGHTS MANAGEMENT (DRM) TECHNOLOGY AND PRIVACY

---

Background to comments made to an Agencies Leaders' Forum meeting at the State Services Commission, 23 March 2005 by Lindy Siegert, Technology Team Leader, Office of the Privacy Commissioner.

Any use of the public (open) packet-switched networks requires that the equipment involved in transmissions, such as a computer's network card, identifies itself using Internet Protocol (IP) addresses. Previously that information was not directly linked to individuals or their personal information. However, users of DRM-protected software or files are typically required to provide personal information that can be linked to that software, its operation, (sometimes) the associated hardware, and even other activities performed at that computer. Registering a software licence with its creator/distributor is the usual method.

A rich source of information about DRM and privacy issues is the Electronic Privacy Information Centre website (<http://www.epic.org/privacy/drm>). Much of what is summarised below is based on material from that site. EPIC have made submissions to the US Department of Commerce separately and jointly with other organizations such as the Samuelson Law, Technology & Public Policy Clinic at Boalt Hall, School of Law, University of California, Berkeley.

In the physical world, anonymous use (if not the acquisition) of media and its intellectual content is the norm – even the purchase of the content can be anonymous if cash is used.

- No-one is aware of the pages you read in the paper, unless they are reading over your shoulder in the train.
- No-one is aware of the pages you re-read in a book, nor do they care if you do so 10 times because the material was complex or you loved the poem.
- No-one is aware of the exact place where you paused the video to answer the phone, how long it stayed paused, or where you re-wound to, once off the phone.

All those actions and more can be tracked by DRM software. DRM software as currently available is capable of:

- Tracking use of the software
- Reporting back to the copyright owner or seller or other party on that use or even other totally unrelated activity on your computer
- Limiting the number of times you can read that page or view that video



Privacy Commissioner  
Te Mana Matapono Matatapu

#### Other Issues:

The “phone home” feature could permit copyright owners and intermediaries to adjust the price you pay for access to DRM protected products according to what they have learnt about you and your habits. DVD zoning already does that to populations of people.

The log files created by DRM software on a user’s computer may be open to examination by spiders or other software agents under the control of others beyond the copyright holder or their agent and without the knowledge of the user.

As the infrastructure to administer most DRM software is outside NZ, those “phone home” transmissions are sent where the protections of the Privacy Act are absent and personal information can be aggregated in ways that are not possible in NZ and that are possibly contrary to NZ cultural norms.

So far, there has been no commercial effort to design privacy-friendly DRM although the IWGDPT called for such development at its meeting in 2000 and there have been proposals put forward at various international meetings of how privacy-friendly DRM systems could be designed.

- International Working Group on Data Protection in Telecommunications, Common Position on Privacy and Copyright Management. Adopted At The 27th Meeting Of The Working Group On 4-5 May 2000 In Rethymnon / Crete. [http://www.datenschutz-berlin.de/doc/int/iwgdpt/co\\_en.htm](http://www.datenschutz-berlin.de/doc/int/iwgdpt/co_en.htm)
- Privacy and Digital Rights Management: An Oxymoron? Information and Privacy Commissioner of Ontario, October 2002. <http://www.ipc.on.ca/docs/drm.pdf>
- Towards Meeting the Privacy Challenge: Adapting DRM, by Larry Korba and Steve Kenny. 2002 ACM Workshop on Digital Rights Management, Held in Conjunction with the Ninth ACM Conference on Computer and Communications Security. Washington, District of Columbia, USA. November 18-22, 2002. NRC 44956. [http://it-iti.nrc-cnrc.gc.ca/publications/nrc-44956\\_e.html](http://it-iti.nrc-cnrc.gc.ca/publications/nrc-44956_e.html)

The operation of DRM services, the surveillance software used, and the licensing regimes are far from transparent or easy for the average user to understand. A group from the Samuelson Clinic, examined these services and had this to say:

“The ways that information is collected and processed during use of the services examined is almost impenetrably complex. It is difficult to determine exactly what data a service collects, and merely discovering that separate monitoring entities sit behind the services requires a careful reading of the services’ privacy policies.” (How DRM-Based Content Delivery Systems Disrupt Expectations of “Personal Use”. Deirdre K. Mulligan, John Han, and Aaron Burstein. Presented at the ACM 2003 Digital Rights Management Workshop .



Privacy Commissioner  
Te Mana Matapono Matatapu

<http://www.law.berkeley.edu/cenpro/samuelson/papers/other/WPES-RFID-p029-mulligan.pdf> )

Some other concerns that while not normally posed as privacy concerns do arise from the potential for constraint of private thought and intellectual exploration. A paper by Julie Cohen, from the Samuelson Clinic, discusses many such issues.

- DRM and Privacy, by Julie Cohen. Berkeley Law Journal, 2003. <https://www.law.berkeley.edu/institutes/bclt/drm/papers/cohen-drmandprivacy-btlj2003.html>

There are concerns about the effect DRM technologies may have on freedom of speech and democratic processes by constraining intellectual exploration through restricting access to content or by the “chilling effect” of tracking and reporting on use. DRM permits the introduction of censorship by and for commercial interests without reference to cultural norms and practices. The existing geographical zoning of DVDs is a model of how this could happen. It has also been postulated that these technologies make possible the recasting of the social contract through piecemeal modification/restriction of consumer behaviour and expectations. Automated decisionmaking is another area of concern as DRM can “punish” as well as constrain and monitor, by for example, detecting an attempt at unauthorised access and refusing it or destroying the copy.