Copyright-related Policy summary for CLUE: Canada's Association for Open Source

The Vision of CLUE is to nurture a Canadian Information Technology environment that promotes collaborative innovation as well as open standards and the rights of consumers.

The Mission of CLUE is to promote the use and development of Free/Libre and Open Source Software (FLOSS), by providing a public voice to the community for its Canadian users, developers and supporters. CLUE will enhance this community's ability to share resources, define standards, and promote its values within Canadian society.

Overall policy focus is to protect the the right of the owners of digital technology to make their own software choices, and further to seek to remove any legal or other barriers that would favour non-FLOSS software over FLOSS.

Petitions: CLUE endorses both the "Petition for Users Rights (in Copyright)" and the "Petition to protect Information Technology property rights" as organized by the Digital Copyright Canada forum. http://digital-copyright.ca

Primary Copyright related concerns:

- We disagree with the legalization or legal protection of techniques used by copyright holders to encode their content such that it can only be accessed with "authorized" technology brands.
- We disagree with the legalization or legal protection of techniques used by device manufacturers to lock down devices such that their owners are considered attackers, where someone other than the owner controls the keys, or where owners are otherwise not able to control their technology for lawful uses or make their own software choices. Hardware owners must be able to make their own software choices, in order to chose our software.
- We disagree with government promotion or mandating of royalty-based business models over fixed-cost based models used in peer production and peer distribution such as FLOSS.

Policy proposals:

- Canada should take the lead from our trading partners and adopt a living "fair use" model. This should include carving out from copyright private activities such as time, space and device shifting of legally acquired content. Canadians should not need permission or payment to carry out these activities that most Canadians already believe is legal.
- Canada should put "clarifying and simplifying the act" as the top priority for the revision process. Many Canadians carry out activities that they believe are legal, but, that the act doesn't allow. Other Canadians believe things to be illegal that are not.
- Canada should clarify and simplify the term of copyright, resisting any proposals to extend and/or obfuscate the expiry date of copyright. For example, the term for photography should be a fixed 50 years from when the picture was taken, and not 50 years from the death of the (most often unknown) photographer.

CLUE: Canada's Association for Open Source http://cluecan.ca
Policy Coordinator: Russell McOrmond http://www.cluecan.ca/mcormond
305 Southcrest Private, Ottawa, ON, K1V 2B7 Last updated: 2008-07-21

- Extended/statutory (compulsory) licenses impose a specific royalty-based business model on all creativity it is applied to. This form of licensing should only be used in extreme cases of market failure, and never in marketplaces where competition is growing. Royalty-free business models are rapidly growing worldwide in software as well as scientific and educational material.
- The 1996 WIPO treaties were primarily aimed at protecting incumbent business models from disruption from competitors (1994/1995 National Information Infrastructure task force in the USA). Ideally, Canada should not implement or ratify these legacy 1996 treaties. Lawyer Howard Knopf <http://excesscopyright.blogspot.com> states that Canada has no obligations here. If ratification is desired, less harmful ways exist to do so.
    - Do not extend copyright to include a new "right of interoperability" where authors can encode their content to only be interoperable with chosen brands of access technology.
    - Ensure that legal protection for technical measures only extend to infringing acts , and not simply "unauthorized" acts. This critical issue was articulated in the 1996 WIPO treaties and the proposed Liberal Bill C-60.
    - Clarify that software is neither a "device" (as interpreted in the USA with relation to their DMCA) nor a "service" (as could be misinterpreted in the context of C-60), and that there would be no prohibition over the authoring, distribution or use of software that had substantial non-infringing uses.
- Intermediaries should not be liable when they are simply acting on behalf of their customers, or providing solutions under the control of customers. The "notice and notice" regime for ISPs proposed in Bill C-60 and Bill C-61 should be retained. Authors of software with non-infringing uses should not be held liable for any abuses of that software to infringe copyright.

Comparison of Liberal Bill C-60 (June 2005) and Conservative Bill C-61 (June 2008)

The key policy for software authors is "technological measures", given this policy is about what software the owners of computers are and are not allowed to install and use on their own hardware. The Liberal Bill C-60 recognized the nuances of the 1996 WIPO treaties and tied anti-circumvention legislation to activities that would otherwise infringe coyright. The WIPO treaties use language such as:

> Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

Being "used by authors in connection with" and "or permitted by law" suggests that anti-circumvention legislation should be tied to infringing activities. Copyright and other laws (including privacy law) should trump technological measures when there is a conflict, not the other way around. By clarifying that the anti-circumvention legislation is tied to copyright, the legislation could also avoid providing any protection for technical measures applied to devices by other than their owners.

The Conservative Bill C-61 only limits circumvention to the "authority of the copyright owner", and appears to protect the anti-competitive locks on content (a new "right of interoperability") as well as

protecting locks placed on devices where the keys are controlled by an entity other than the owner. Bill C-61 at least does not protect technical measures applied to content without the permission of the copyright holder, a practise that has been too common.

Jurisdictional issues

What "technological measures" protect is not really copyright directly (see additional notes below), but the secrecy of a message, digital signatures, digitally encoded contracts, and the security of information technology. Contract, electronic commerce and property law are provincial jurisdiction. Many of the unintended consequences of having legal protection for "technological measures" in copyright law, such as protecting foreign locks against the owners of property, could be avoided by modernizing the appropriate provincial laws rather than confusing federal copyright law.

Language/technology issues:

There are many misconceptions about terms such as Digital Rights Management (DRM) and Technical Protection Measures (TPMs), which are used to mean different things by different people.

Technical people talk about technologies, such as cryptography, that can be used to protect the authenticity, integrity, and privacy of information, as well as ensure that only authorized access to computers and data are possible.

Cryptography is the strongest of the technical protection measures. Cryptographic protection only works if the intended recipient of content and an attacker trying to gain unauthorized access to the content are different people. It doesn't work when the recipient and attacker are the same person, as is the case with, say, "protected" digital music downloads. The content cannot be both accessible and inaccessible to the same person at the same time.

DRM proponents talk about the way in which they want to encode content such that it can make various decisions (only allow to be read 5 times, "self" destruct after a certain amount of time, etc). Content does not become "magic" when it is digitized. Digital content can no more make these decisions than a paperback book can read itself out loud. All the logic that can be encoded in content must be carried out on a device. We are creating a conflict between the instructions given to a device by its lawful owner and the instructions given to it by some third party. Computers simply follow instructions, and have no way to resolve this type of conflict.

Back in 1965, Ralph Nader was explaining to the US congress that with an automobile accident there are two collisions: the car hits something, and the passenger hits the car. While automobile safety up to that point concentrated only on the first collision, it was quickly understood that safety features should concentrate on the second collision. This gave us dashboards that weren't made out of metal, seatbelts, air bags, and other such second-collision safety features. The same issue exists for "technological measures" where policy makers have been confused into thinking there is only one "digital lock" being discussed, when there are two: a lock being applied to content, and a lock being applied to devices. It is the lock on devices that they are less aware of that is the source of most of the controversy.

Two important policy questions need to be asked about the use of technical measures: Who is deciding what is "authorized", and is the owner "authorized" to access and control their own hardware? We should not be enacting laws that allege to protect copyright at the expense of protecting tangible property rights.

In any policy analysis we must separate the 4 possible owners involved in digital communications technology: content, media, hardware, software. This is required to ensure that the policy does not reduce the rights of one owner in order to allegedly protect the rights of another. (See: Protecting property rights in a digital world http://flora.ca/documents/digital-ownership.html)

Protecting legitimate business models

Many of the proponents of this policy direction suggest it is needed to protect new business models. Protecting digital locks applied to devices by other than their owners creates a new legal relationship that is not like "ownership", "rental", or other established business relationship. These business models which copyright holders may wish to explore can be protected without the harmful unintended consequences of the current policy direction, simply by harnessing existing legal relationships.

Cell phone and video game companies have been wanting to offer a cell phone or game console below cost, with the idea that they could recoup that cost as part of an ongoing service. This same business model could be protected through a clear service contract or rental contract, possibly including a "rent to own" scenario where the device is eventually unlocked. In this case the owner of the device would be the cell phone or video game provider, and thus locking it to protect the interests of its owners should be legally protected. They should not be legally allowed to allegedly "sell" something where they retain the keys to any digital locks that lock down the device.

Other proponents wish to offer the rental of content where they do not also rent the hardware. This is not technologically feasible, so providers should enforce this arrangement in contracts (rental contract clearly indicating when the content must be deleted) or abandon this business model where there is no physical medium to be renting. There are alternative scenarios that offer the same business value, such as what Rogers Cable has done with their 'Rogers on demand' service.

Rogers and other similar providers should clarify their business relationship. For most of their customers they are renting the hardware, and thus having a Rogers lock on the hardware to protect it from unauthorized access/control (including denying the person renting the hardware) is appropriate. For some customers they allege to "sell" the digital tuner or digital video recorder, and yet do not transfer to the owner the digital keys to any digital locks.

In all circumstances we must protect the legal right of the owner of a device to unlock what they own, in order to place their own locks to secure it from unauthorized access or control.