Access Control Technologies
(Digital Rights Management)

DEF: Access in the digital context, and controls over it, concerns digital content – within the meaning of ‘works’ as per the → Intellectual Property (copyright) system and including also content in databases protected under the sui generis right, excluding therefore the physical world, software per se and hardware. Consequently, this entry is about controlling access to such digital content. According to the Internet Security Glossary, ‘access’ means ‘the ability and means to communicate with or otherwise interact with a system to use system resources either to handle information or to gain knowledge of the information the system contains’, and ‘access control’ means ‘a process by which use of system resources is regulated according to a security policy and is permitted only by authorised entities (users, programs, processes, or other systems) according to that policy’. While the technical parts of access controls (identification and authentication, identity management, technical measures) are of no interest here, Digital Rights Management (DRM) is a term that may be used interchangeably with Access Control Technologies for the purposes of this entry, both denoting technologies that are used to restrict the use of digital content.

INSTR: Digital content is protected by (copyright) law and a right to access it without the rights holder’s permission (meaning reimbursement) is only permitted in rare cases and under exceptional circumstances (for instance, academic or library purposes or system interoperability). Access Control Technologies effectuate this system through technical means. In a way they constitute a ‘by design’ system or a rights holder-imposed system architecture or, even further, an application of the ‘code is law’ ideas into the Intellectual Property (IP) rights realm. As such, they ought to be perceived in principle as lawful (see Article 11 of the WIPO Copyright Treaty, introduced in the EU by the EU Copyright Directive, on Technical Protection Measures). Nevertheless, the fact remains that they are designed and implemented by rights holders without any state or other ratification as to the rules they force upon users. In fact, DRM technologies have been accused of enforcing unlawful business practices by technical means (see, for instance the Apple and SONY BMG class action lawsuits). Among others, DRM implementations have drawn criticism on the basis that they rarely adhere to the pro-user basic IP law principles of ‘fair use’ (in the USA) or ‘private copy’ (in the EU), as well as to the IP doctrine of the first sale (they attempt to regulate the sale of ‘used’ IP). Accordingly, the CJEU has ruled that ‘those measures must be suitable for achieving (their) objective and must not go beyond what is necessary for this purpose’.

CONCL: Access Control Technologies, while useful in enforcing IP rights in an on-line environment of mass unlawful downloading of proprietary digital content, are prone to unlawful implementations, because they are designed and implemented by rights holders alone. Users and the public are generally suspicious of their ‘false neutrality’, because they constitute enforced measures they cannot escape or negotiate. Stricter regulation and monitoring is imperative in order to achieve a balance of protecting both rights holders’ and lawful users’ rights and interests, according to the principle of proportionality, as prescribed by the CJEU.

REFERENCES:
NINTENDO v. PC BOX (CJEU 23/01/2014, C-355/12).
Paul de Hert and Vagelis Papakonstantinou

Administration
(Public Cultural A.)

DEF: Public cultural administration refers to all structures and behaviour affecting the fields of