REPORT ITU-R BT.2036

The problem of unauthorized redistribution of broadcast content* via the internet**

(Question ITU-R 101/6)

(2003)

This Report is a first attempt of addressing the general topic of unauthorized distribution of content over the Internet, and will be updated as further information is provided.

There is a multiplicity of sources from which content can be acquired and redistributed. However, the emphasis is placed here on broadcasting as this information is provided for the attention of the ITU Members of the Radiocommunication Assembly.

What follows is preliminary information that does not pretend to necessarily represent views otherwise expressed in other groups of interest, such as other broadcasting unions working on this subject and from whom contributions are expected in the future.

With the transition from analogue to digital distribution methods, the ability to redistribute broadcast content is greatly enhanced. While some immediate redistribution of broadcast content may be desirable and beneficial, unauthorized redistribution may devalue the original content and/or distribution timing. Pay-per-view and commercially paid programming are examples of archival content which may enjoy further revenue possibilities if protected from unauthorized redistribution over secondary digital networks. As public communications systems expand, such as broadband Internet and consumers gain access to affordable appliances that can manage digital content and can connect to such communications systems, redistribution over the Internet, in particular of premium content, is expected to increase dramatically. Due to the interconnections of digital communications infrastructures, solutions to this problem will require carriage of information across various communications methods and will require the cooperation of multiple industries.

---

* Original report provided by North American Broadcasters Association (NABA). NABA is made up of national broadcasters in Canada, Mexico and the United States of America.

** Working Party 6M will concentrate on technical means to prevent unauthorized distribution of content. Further contributions on this issue are invited from Members.

The unauthorized use of content is not a new problem. There are numerous examples of these trends due to it being easy, quick, and undetectable.[1] With the advent of digital technologies for the storage and communication of content, along with the broadening interfaces of one digital transport mechanism to another, the unauthorized use of content has risen to an all-time high, as observed by North American rights holders.

Many technological advances have created an environment where digital signals and content can be distributed simply and rapidly, often without knowledge of whether this distribution is authorized or not. The reception of content in a digital format allows the content to be replicated in the consumer domain at a reasonable quality and in a significant number of generations. As a result, difficulties that pirates may have had in creating good-quality video on analogue media, no longer exist. The rapid decrease in the cost of computing power and digital storage has put unauthorized digital copying capability in the hands of the general public, such that copying of content no longer requires the physical acquisition of professional equipment.

New advances in compression provide improved quality in smaller digital packages. The convergence and interconnectivity of many digital communication and storage media allows convenient transformation and movement of signals from broadcast sources to compact storage media, such as DVD, and on to communication channels, such as WiFi and Ethernet, transparently around the world. Increased wired capacity, advancements in peer-to-peer file transfers, among others, are all resulting in the ability to access content without authorization in as little time as it takes to make a phone call connection around the world. The increasing availability of broadband in both corporate and home connections means that signals and content may be moved by a majority of consumers. While a full digital broadcast signal may be cumbersome to move across Internet connections today, compressed versions of broadcast content are being posted to the Internet on a daily basis. It is a mere matter of years before full high-definition signals will be able to be exchanged easily.[2]

Today, using consumer-grade equipment, increasingly available in homes throughout the world, one 10-year old child can move the equivalent information of a broadcast signal to millions of worldwide peer-to-peer users in less than an hour after the broadcast, which can result in the loss of broadcast television viewership, not only in the immediate global windows of first-run television, but also in the syndicated broadcast market.

---

[1] Sources of information on digital content theft include:

- Based on search results for six analogue terrestrial broadcast television programmes from the MPAA's Internet anti-piracy search firm, Ranger Online, the growth of illegal file trafficking in television programmes increased over 600% from 2001 to 2002.
- In the year 2000, a company called iCrave TV was shut down for the unauthorized retransmission of United States of America and Canadian signals over the Internet.
- A quote from the BBC News Online, 7 May 2003, stated, "On Monday I watched the latest episode of ER just a few days after it was broadcast in the US ... which I had downloaded from the internet ... almost all the programmes had been broadcast less than a day earlier in the US, many months before viewers in the UK and Europe will see them".

[2] According to Probe Research in 2001, end-user broadband connectivity rates were increasing at approximately 50% per year, and typical end-user broadband connectivity that year was approximately 0.6 Mbps. If trends continue at this pace, a full high definition television (HDTV) signal could be redistributed to the Internet in real-time by the year 2010.

It is important to understand that protection of digital content will never be perfect and, thus standards should be designed to keep unauthorized use of content to a level that can be reasonably enforced through legal avenues. Standards should neither impose unnecessary restrictions upon a viewer's ability to access and enjoy digital broadcasts as they do analogue broadcasts, nor prevent the use of legacy devices. Looking at the models of physical content protection, it should be anticipated that those standards would include various methods of protecting rights. It is possible and likely that some content may be protected by more than one method. It is probable that, as with every type of physical lock after some period of time, any individual protection method may become easy for the common citizen to bypass, increasing the probability of unauthorized use of content and, therefore, requiring upgrades in the technical protection mechanisms.

Solutions must be developed that allow broadcasters to take advantage of secondary redistribution while protecting such redistribution from misuse of the content or distribution rights, if required. Radiocommunication Study Group 6 is an appropriate venue to study and make recommendations for solutions that enhance and protect broadcast content in a way that also ensures that this protection is maintained when the content leaves the broadcast domain.