



WHITE PAPER



DIGITAL SERIAL NUMBERS AND PIRACY DETERRENCE
THE DETERRENT EFFECT OF DIGITAL SERIAL NUMBERS ON ILLEGAL
FILE-SHARING AND DOWNLOADING

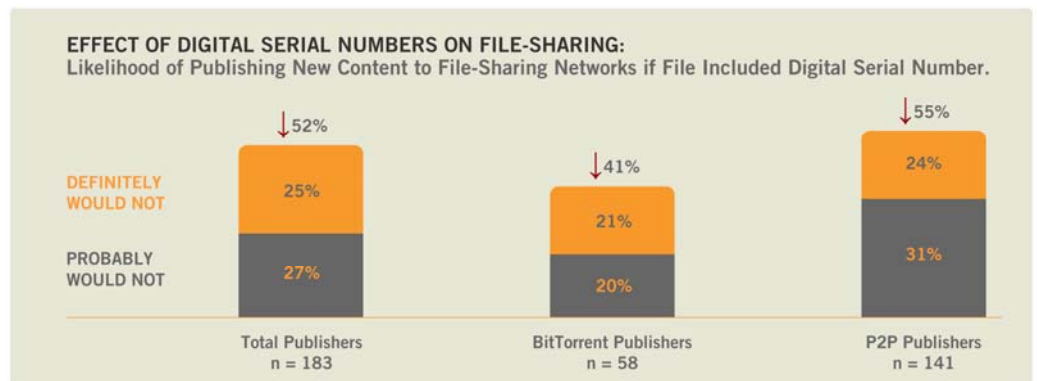
SUMMARY


Digital piracy is commonplace: Most consumers who download entertainment media acquire some of it illegally. The precise economic cost to content owners of digital piracy is unestablished, but many studies have estimated it to be substantial.

Deterring digital piracy poses both technical and cultural challenges. Digital rights management (DRM) systems have proven inadequate in both respects. Technically, DRM systems can be subverted through various means. And in the culture of media consumers, they are widely thought to be overly restrictive.

Digital serial number (DSN) systems represent an alternative response to digital piracy. A DSN is a form of *digital watermark* — a unique code embedded imperceptibly in digital content. Like a physical serial number, a DSN establishes the provenance and ownership of the numbered item. DSNs can be used to track content to deal with illegitimate file sharing, but an even greater benefit may derive from using them as a deterrent to piracy.

Prior to deploying DSN systems, content owners require some assurance that they will have a deterrent effect. This paper reports on a survey commissioned by the **Digital Watermarking Alliance** that investigates this question. The survey, *Consumer Strategies for Deterring Illegal File-Sharing Using Digital Serial Numbers*, assesses current behaviors regarding illegal sharing of media and determines how behavior would change if consumers were aware that digital media could be identified through DSNs.





The survey's results confirm the conclusion that DSN systems would have a strong deterrent effect on digital piracy:

- Illegal downloading would decrease significantly among all downloaders.
- Both intentional and passive file-sharing would decline by about one-half overall.
- A small but noticeable number of media consumers would increase their purchases of physical media.

This deterrent effect requires that consumers are aware that DSNs are present in digital media, so adoption of DSNs must be accompanied by programs or consumer education. Such programs have good prospects of effectiveness because, as the survey reveals, consumers generally view DSNs as an unintrusive approach to balancing the rights of content owners and consumers, so such programs have good prospects of effectiveness.

INTRODUCTION


The entertainment industry faces a challenging environment. The production and distribution of entertainment media (music, TV, and movies) by digital means, while beneficial to the industry, has also made *digital piracy* — the illegal sharing of entertainment media — significantly easier. While consumers continue to buy physical media and purchase media online, a significant proportion of consumers also participate in the illegal sharing of media through peer-to-peer (P2P) networks and file-sharing applications such as BitTorrent.

While the economic scope of this problem has not been precisely quantified, its negative impact on the entertainment industry is undeniable. Consider these examples:

- A pre-release version of *X-Men Origins: Wolverine* was posted to a file-sharing site on the internet from which it was downloaded an estimated 100,000 times. (*BBC*)
- There were approximately 350,000 downloads of pre-release tracks of the much anticipated Guns N' Roses album *Chinese Democracy* from a music writer's blog. (*Mediapost.com*)

While illegal downloads do not equate one-for-one with lost sales, it is likely that a portion of the 450,000 downloads represent consumers who would have purchased a ticket to *X-Men Origins: Wolverine* or a copy of *Chinese Democracy* once they became publicly released, in the absence of an opportunity to acquire it online for free.

Digital piracy is commonplace. More than four in five consumers who download content do so illegally at least some of the time. While almost half of those consumers also download content legally, that leaves less than one in five consumers who download



More than four in five consumers who download content do so illegally at least some of the time.



content strictly legally. These numbers do not indicate how many actual downloads are illegal overall, but they strongly suggest that legal downloads make up the smaller portion by far.

This is clearly a situation the entertainment media industry would like to change. The question is: how?

DETERRING DIGITAL PIRACY

The difficulties in deterring digital piracy are two-fold: technical and cultural. The technical difficulty is developing a technology that balances content ownership rights with the fair use and ease of distribution of content.

The cultural issues include an increasing acceptance of illegal downloading and sharing as a legitimate means of acquiring media, the belief that individuals are unlikely to be caught engaging in piracy, and resistance to the overly strict constraints of digital rights management (DRM) systems.


In general, DRM systems operate by protecting content with some type of technical barrier that can be unlocked only on a specific device or small set of devices. For example, digital music may be encrypted when it is purchased such that it can be decrypted and played only on specific devices identified at the time of purchase.

DRM systems have been deployed with little real success, and the failures have been both technical and cultural in nature. Technically, DRM systems can be subverted by direct attack on the technical barrier or simply by capitalizing on the *analog hole*. The analog hole exploits the necessity for converting digital content to analog form — actual light and sound — for enjoyment, and in the analog state it can easily be re-recorded free of DRM constraints. Culturally, DRM systems have been perceived by many consumers to be overly restrictive and encroach on legitimate and fair uses of content.

DIGITAL SERIAL NUMBERS

A different approach to deterring digital piracy employs *digital watermarks*. A digital watermark is data embedded in content in a way that is imperceptible to human senses but easily extracted by digital devices. Within its size constraints, a digital watermark can contain virtually any information required by the application at hand: copyright notices, date-time stamps, MPAA ratings, etc.





In the context of digital media watermarks can be used to embed unique codes to identify individual embodiments of content — individual copies of digital movies, broadcasts of TV shows, copies of music CDs, etc. Digital watermarks used in this way are effectively *digital serial numbers*, establishing the identity and ownership of individual embodiments of digital content.

Serial numbers are widely understood and an accepted phenomena in both the physical and digital worlds. Most objects of value are serial-numbered to establish their provenance and to provide a variety of benefits to both consumers and manufacturers. In the physical world, objects ranging from cars to cameras to computers are serial-numbered. In the digital domain, software applications and video games are serial-numbered. Digital watermarks extend the application of serial numbers to digital content.


DETECTING DIGITAL PIRACY, PART II

The digital serial number (DSN) enables a different approach to deterring digital piracy, an approach that is less coercive and more cooperative than DRM. DSNs do not prevent any particular use of digital media. Instead, DSNs enable digital media to be tracked and identified so that illegitimate uses can be detected and dealt with appropriately as the content owner determines. Legitimate uses of content are not restricted in any way.

DSN systems also allow content owners to determine where the bulk of misuse of content occurs. This information enables content owners to craft win-win solutions that serve the interests of content owners and consumers alike — delivering content to consumers when, where, and how they like, while also providing compensation to content owners.

In a DSN system, individual embodiments of content are serial-numbered at some point prior to public dissemination. Disseminated content can then be filtered and identified at known transit points (e.g. YouTube) or screened and identified at other points where it appears unexpectedly (e.g. blogs). Once content is identified, there is an opportunity for the content owner to assert the rights of ownership. For example, in the two scenarios briefly mentioned above, the existence of DSNs would enable tracing the original copy of *X-Men Origins: Wolverine* that was leaked or substantiating a claim of damages against the blogger who posted cuts from *Chinese Democracy*.

Perhaps the biggest benefit of DSNs is the potential for deterring unauthorized uses of content rather than enforcing ownership rights after the fact of misuse. DSNs clearly imply to consumers that the content they've acquired carries legitimate ownership rights. In addition, DSNs enable content to be tracked so that the source of shared content can potentially be identified. In this context, consumers are likely to be more circumspect about both acquiring and sharing content freely. However, the effectiveness of DSNs as a deterrent requires that consumers be aware of their presence and legal significance. This is the cultural component of deterring digital piracy: educating consumers about DSNs.



DSNs clearly imply to consumers that the content they've acquired carries legitimate ownership rights.





CONSUMERS AND DIGITAL SERIAL NUMBERS

Consideration of DSN systems raises questions for content owners. For example, implementing a DSN system requires some up-front investment in infrastructure to embed watermarks in content. Also, content owners must consider legal questions, policy changes, enforcement mechanisms, and privacy issues. So before undertaking the changes necessary to adopt DSN systems, content owners will naturally ask: How do we know that digital serial numbers will help deter piracy?

A survey was commissioned by the **Digital Watermarking Alliance** to answer this question. The survey, *Consumer Strategies for Deterring Illegal File-Sharing Using Digital Serial Numbers*, was designed and executed by **Interpret, LLC**, a global research consulting firm focused on evaluating and measuring the intersections of media content, technology, advertising, and consumer behavior. The survey polled a meaningfully large sample of U.S. consumers who share entertainment media. The survey assessed current attitudes and behaviors with respect to sharing and then determined how those attitudes and behaviors would change in the context of DSNs. The following discussion summarizes the results of this survey.

CURRENT ATTITUDES AND BEHAVIORS

Consumers who download entertainment media engage in a variety of both legal and illegal downloading activities. The survey identifies three overall groups:

- *Legal-only downloaders* acquire media strictly legally.
- *Hybrid downloaders* acquire media both legally and illegally.
- *File-sharers* acquire media only through illegal downloading and file-sharing.

Legal-only downloaders are a small minority of all downloaders — fewer than one in five. Hybrid downloaders make up fewer than two in five. So, file-sharers constitute almost half of all downloaders. As mentioned previously, digital piracy is commonplace.

Of the hybrid downloaders and file-sharers, three-quarters use standard peer-to-peer (P2P) networks, about half use BitTorrent, and about one-quarter use both. In a standard P2P network such as GnuTella, peer nodes operate without central servers to pass requested files intact from source to destination node. BitTorrent is a P2P protocol that is better for very large files. It enables many nodes to work in parallel to transfer a requested file in pieces to be reassembled at its destination. BitTorrent requires more effort to use, and its users tend to be more committed to the notion of file-sharing.

Consumers who share digital media fall into two broad categories:

- *Passive sharers* are those who distribute media by not taking action to prevent it.
- *Active sharers* are those who knowingly distribute media via file-sharing and P2P networks.

Passive sharers usually become distributors inadvertently by, for example, leaving downloaded media

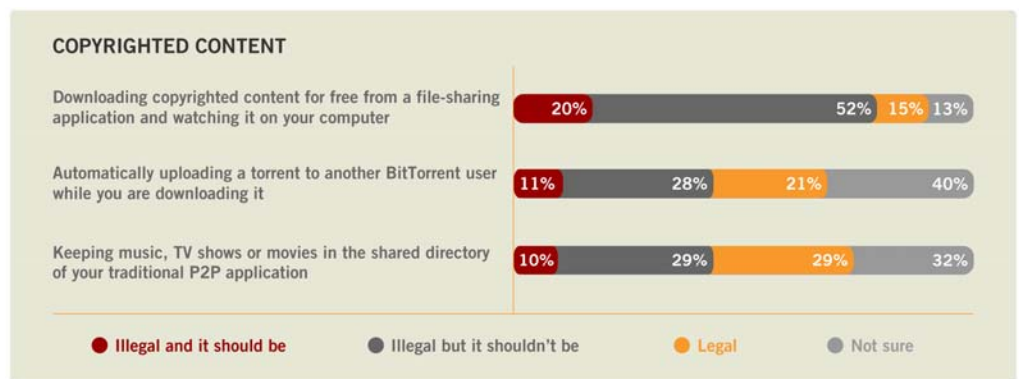


files in a folder that's publicly available on a P2P network. In many cases, passive sharers simply do not understand how their file-sharing applications work and are unaware that they are a distribution source.

Consumers download from file-sharing applications for a number of reasons (listed in decreasing order of importance):

- It is the easiest way to access digital entertainment media.
- Consumers can't afford the retail price of entertainment media.
- There is content available via download that isn't otherwise readily available.
- It is easier to find desired content.
- It is easier to transfer content to other digital devices.
- Consumers can collect content that they wouldn't buy.
- Digital media is preferred to physical CDs and DVDs.

More than three-fourths of consumers know that it's illegal to acquire or share copyrighted material without purchasing it. But significant numbers of consumers think it should be legal — from one-quarter to one-half depending on the situation.



Current attitudes and behaviors show a high incidence and tolerance of digital piracy, but they also reveal areas where consumer anti-piracy education may have an impact. In particular, hybrid downloaders may be swayed towards more legal downloads, especially if some of the reasons why they download illegally — ease of use, availability of content, etc. — are addressed. Also, passive uploaders could be motivated by anti-piracy education to manage their own media files more safely.

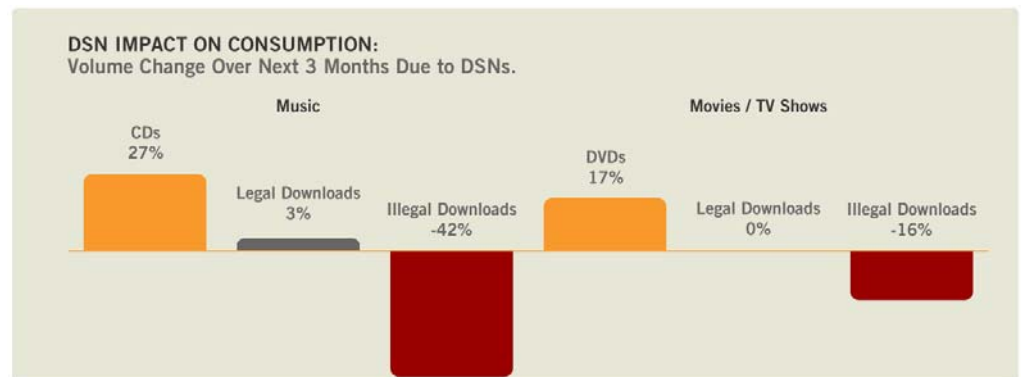
ATTITUDES AND BEHAVIORS IN A DSN ENVIRONMENT

To determine how behaviors and attitudes would change in an environment of digitally serial-numbered media, survey participants were asked to respond to a variety of different scenarios after DSNs were explained to them. The explanation specifically contrasted DSN and DRM systems to emphasize that Digital Serial Numbers “do not place any limitations or restrictions on where and how you can use

content originally bought online” and “will not interfere with your ability to use the content as you like for your personal enjoyment.” Participants were also informed of the benefits of DSNs to content owners — that copyright holders could, for example, track the origin of a movie made available through BitTorrent.

The results of the survey show that four out of five consumers generally agree that DSNs provide a solution that is “less cumbersome,” “a better balance between consumer needs and copyright protections,” and “give [consumers] more freedom than DRM.” In addition, the numbers reveal the deterrent effect of DSNs:

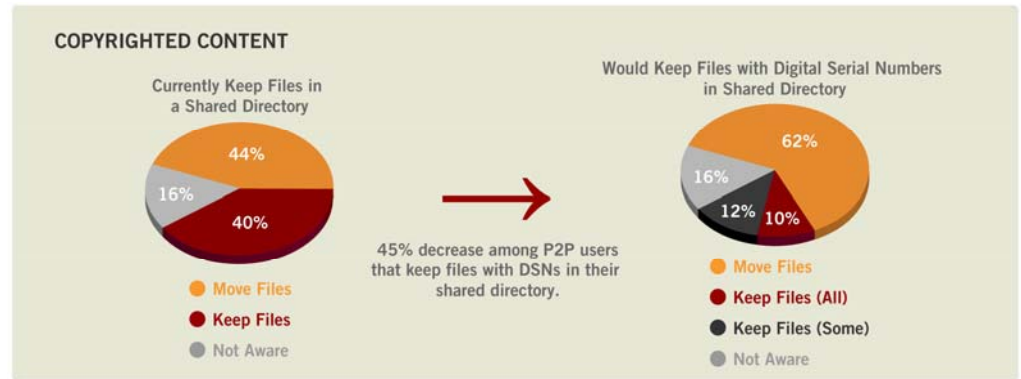
- Illegal downloading via file-sharing applications would decrease by one-third among all downloaders, with a slightly larger reduction among file-sharers.
- Active sharing via file-sharing applications would decline by one-half overall, a little less among BitTorrent users, a little more among P2P network users.
- Passive publishing via P2P networks would decrease almost half among those who previously chose to leave files in shared folders.
- Among all consumers, a small but noticeable number — fewer than one in five — would increase their purchases of physical media (CDs and DVDs).



The deterrent effect of DSNs is supported by these results, but there are consumers for whom DSNs would have no effect on their illegal downloading. More than one-half of file-sharers would illegally download at least the same amount for the following reasons (listed in decreasing order of importance):

- I don't download enough to be caught.
- The online community will remove DSNs.
- DSNs will not be enforced strongly enough to make a difference.
- My downloading would remain the same as a statement of principle.
- The BitTorrent community can avoid sharing files with DSNs.

- The risk is worth it.



Interestingly, DSNs would have a mild positive effect on the legal online purchases of entertainment media: one-quarter of all legal downloaders would increase their online purchases, though only by modest amounts. Why would DSNs cause an increase in online purchases among those who were already purchasing legally? One reason may be that DSNs are perceived as being less restrictive than DRMs, so that consumers have freer use of their legally purchased content.

CORROBORATING RESULTS

Other surveys support the proposition that educating consumers about illegal downloading can have a deterrent effect. A survey conducted in the U.K. and France by **The Leading Question**¹ showed that more than three-fifths of respondents would stop downloading music illegally if their ISP sent them a warning letter. A similar survey by **Entertainment Media Research**² reported comparable results: Seven in ten consumers would stop their illegal downloading after a single warning from their ISP, with the number approaching eight in ten among younger consumers. While neither survey directly addressed the concept of DSNs, they support the contention that it can be effective to educate consumers about rights and responsibilities regarding digital media.

CONCLUSION

DSN technology promises to be effective in deterring digital piracy, but it can work only if consumers are aware of the presence of DSNs in digital media. The rollout of DSN systems should be combined with campaigns to educate consumers on how copyright laws apply to downloading and sharing digital content.

This survey suggests that consumers view DSN systems as a balanced approach to satisfying the needs of consumers and content owners alike, so such education campaigns seem likely to be well-received. Particular impact can be achieved by educating passive sharers to their obligations and risks, as well as how to prevent passive sharing.

¹ The Leading Question, www.theleadingquestion.com

² Entertainment Media Research, www.entertainmentmediaresearch.com