MEDIA & ENTERTAINMENT

Chain of Custody: Risks, Security, Costs and Ensuring That Your Content is Safe for Media and Entertainment

The National Institute of Standards and Technology (NIST) defines Chain of Custody, Provenance and Immutable as:

Chain of Custody	*"A process that tracks the movement of evidence through its collection, safeguarding and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer."*
Provenance	*"In the context of computers and law enforcement use, it is an equivalent term to chain of custody. It involves the method of generation, transmission and storage of information that may be used to trace the origin of a piece of information processed by community resources."*
Immutable	*"Data that can only be written, not modified or deleted."*

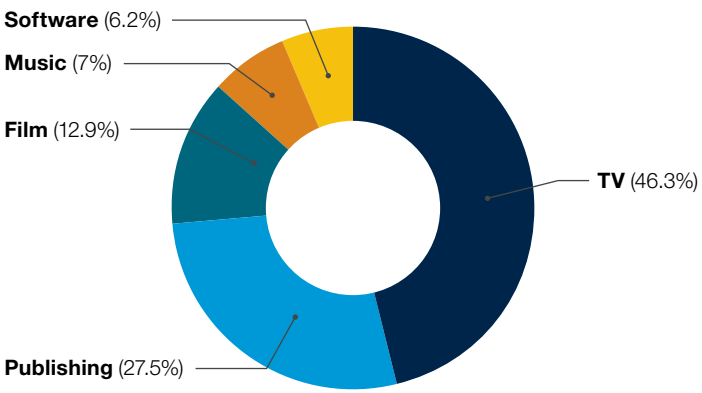
Why Is Establishing a Clearly Defined Chain of Custody So Important?

We are all quite familiar with the importance of establishing a chain of custody as it relates to evidence in a legal procedure. In any such investigation, it must clearly be established and proven that evidence presented in a court proceeding has remained unchanged from the time that it was first gathered. Alternatively, in the sports world, the drug testing of athletes must include an established process that ensures that samples are tamper-proof. Failure to ensure a documented chain of custody could result in drastic consequences for individuals and corporations.

Heretofore, in the Media & Entertainment (M&E) industry, activities around the security of content have mainly focused on anti-piracy measures. These actions have included a variety of technologies such as digital rights management (DRM), fingerprinting, watermarking and take-down notice issuances, but, by and large, content piracy continues to result in multi-billion dollar losses.

Today, however, there is an entirely new set of complications which has made it critical for the M&E industry to establish rules and procedures to ensure that a chain of custody be a priority in the content creation-to-consumption cycle.

Share of 2022 Global Piracy Traffic



Source: Variety

! With technology that creates seamless lip synchronization, phoneme substitution, facial characteristic alteration, etc., we are now experiencing critical questions of whether what we hear and see are real or have been artificially created or altered.

Is Securing the Content Sufficient Enough for a Chain of Custody Process?

As file-based aggregation and distribution systems replaced other methods and high value content now being moved as packets across networks, it was clear that any type of content could be transmitted in this fashion. However, the below witness testimony makes it clear that solely securing content was insufficient and that a non-repudiation chain of custody must also be established.

Witness Testimony (Product Development Manager shares his experience of establishing a chain of custody)

"In 2010, I was responsible for product development at a managed file distribution company, and we were asked by a global news organization to transmit genocide witness testimony that would eventually be used in court proceedings. This was an extremely serious matter. Unless it could be proven that a chain of custody was established from point of origin to point of destination and that the files sent were the exact, non-altered and non-hijacked files, there was every possibility that these testimonies would be inadmissible in court.

We solved this problem with the use of an extensive list of technologies and procedures that passed the security questions and legal issues that had to be addressed. The result was the successful transmission of files which maintained and documented a chain of custody. We could show every network path that the files took with specific timestamps, how origin and destination servers were mutually authenticated and, finally, how hashing algorithms proved that the file hashes were exact from point to point. We also had to produce logs of file payloads, as well as specific access control settings and authorized personnel credentials. All of this was being monitored in both near real-time and real-time."

Supply Chain and the M&E Industry: Security, Auditing and Copyright Infringement

As per the above Witness Testimony example, there is a great need for establishing an immutable chain of custody. But what about the applicability to the M&E industry? For M&E, there are three obvious areas that rise to the top—security, auditing and copyright infringement.

During the 2010-2023 timeframe, the standard process of shipping hard drives, videotapes or even film canisters was replaced by file-based aggregation and distribution systems. Files representing the images and sounds of the world's most expensive per second content traverse global networks as content production teams work around the clock and across the world. With the compressed time schedules for making and delivering content, file-based systems and workflows have transformed the digital media supply chain.

With the proper safeguards in place, content can be secured, content access can be audited and copyright infringement can be reduced. A number of solutions need to be employed in order to establish provenance, immutability and a provable chain of custody. Below, find an industry-applicable example where several areas were addressed by employing multiple technologies.

From 2001 to 2004, a period of massive concern gripped the music industry, especially related to unauthorized music file sharing sites, piracy and the leaking of pre-release music. Additionally, it was a routine process to use overnight delivery services to send compact discs (CDs) to various outlets. However, this presented a series of problems that music labels needed to address:

- **How could a day and time embargo be implemented for radio stations?**
- **How could overnight shipping receipts be coordinated to prove that every station received its package?**
- **Could there be a way for content to be encrypted only for an individual (station) recipient?**

This particular problem was addressed by:

- **Creating a client-server architecture**
- **Encrypting and decrypting content on the fly during playback**
- **Rotating encryption keys on a variable basis**
- **“Unlocking” access to content when digital receipts were received such that same day and time delivery for all participants could be achieved**

These changes resulted in increased efficiencies and security, auditable asset tracking and a reduction of the supply chain from three weeks to nine days. What is important to note is that multiple layers of technology were required to adequately address the issues.

Key Considerations for Media Organizations When Evaluating a Chain of Custody Process

To establish an effective chain of custody process, clear procedures must be in place, encompassing proper documentation, detailed records, timestamps and signatures–all of which are essential at each stage of the process. However, various challenges can hinder the smooth execution of the process, making the endeavor cumbersome. Let's explore a few key topics to consider:

How Deep Fakes, Alterations and Generative-AI Can Impact Content Quality

In the M&E industry, technology can be utilized to create amazing characters and visuals to tell engaging and delightful stories. However, it is clearly becoming more difficult to ascertain whether content is original, artificial or altered. In order to establish and maintain a chain of custody for content, it is not just a matter of putting technology to use. Instead, a range of methods utilizing technology, best practices and physical and virtual security procedures must be present.

A number of technology companies have begun initiatives intended to classify and protect the provenance of imagery with the goal of verifying if content was created with a Generative-AI application. Further, establishing the origin of content and ensuring that the content has not been altered is an important aspect of these initiatives.

Watermarks Alone Are Not Sufficient

In the world of print media and broadcast, the use of visible and invisible watermarks has long been the status quo for identifying and establishing ownership. However, watermarks are not infallible and are susceptible to any number of methods of being rendered illegible.

Newer methods will include cryptographic signatures along with specific metadata creation to indicate the origin and original state of the content. With these approaches there exists the concept of a writer and a reader—a form of technology bundle in which a writer identifies characteristics and a reader enables the discovery of those characteristics. One example of a specification for writing and reading of these signatures is the Coalition for Content Provenance and Authenticity (C2PA). While this is a standard, in these early days of Generative-AI, will other approaches and potential "standards" be forthcoming?

Digital Fingerprinting at the Camera Source

An additional technique is to introduce digital fingerprinting at the source of content capture—at the camera level. As content is being captured, it can be digitally fingerprinted. This will establish a unique digital identifier relating to the integrity of each unit (frame or sub-frame) of content.

Digital fingerprinting is, essentially, a unique digital representation of audio and video based (often but not exclusively) on the sonic characteristics of audio and the optical characteristics of video. As with human fingerprinting, these are unique and will change given the naturally occurring variations in recorded or streamed audio and video. Depending upon the implementation, one can easily imagine a camera manufacturer providing an in-camera digital fingerprinting algorithm that marks each "sampling" of audio and video.

Naturally, these fingerprints must be treated as if they were keys to a set of locks. Fingerprints can be encrypted and maintained in a tamper-proof hardened storage module. While much of this computation may not occur at the camera-level, the fingerprints can be stored or transmitted along with the video. Fingerprints can then be used to identify and retrieve content. Most importantly, they are used to identify if an original frame's fingerprint has been altered, thereby calling into question whether the frame has been modified in some way.

Another Way of Thinking About Encryption

When files are being aggregated and distributed across any network and deposited in a storage system, status quo dictates that content will be "encrypted in transit" and "encrypted at rest." However, an additional requirement that is going to take on increased importance is the concept of encryption of content in-use. It is obvious that today, when a file is accessed from storage where it is in an encrypted form, that file is decrypted in order to be "read" and used. When that occurs, there is always a danger of the file being altered in some way which may impact its authenticity.

What is needed is a methodology by which content can be manipulated (used) while staying in an encrypted form or, failing that, within a secure environment. One method is to implement a hardened security module which contains cryptographic keys to "unlock" the content and that is tamper proof. While this may seem to some as "overkill", we will eventually need to determine when this approach is necessary and how best to implement.

Blockchain Integration

The use of a blockchain is yet another solution that provides immutability and a record of all transactions. Blockchain's decentralized nature offers great capacity and uses a distributed and public ledger. Once a transaction has been recorded, it cannot be altered unless every subsequent block in the chain is altered, which cannot occur without network consensus.

Ensuring Unalterable Integrity: Immutability

Immutability refers to data that can only be written and not modified or deleted. Ensuring and proving that data is immutable is a key concept in content custody. Informative work was done in this area as part of the "News Provenance Project," which used blockchain's data structure "to maintain a transparent and immutable record of a photo's origin."

Establishing and guarding the provenance and immutability of content provides the much needed context of what the content is, its origin, the circumstances of its origin and the path that the content has taken from its origin point to its various distribution points. Blockchain, with its distributed ledger, tracks modifications or additions and thus is an appropriate, but not an exclusive, choice.

Today's Content Now Exists as Files

With the exception of non-digitized film, almost everything we see and hear now exists in some format on storage subsystems.

> Today, there is still the ongoing issue of a majority of the world's largest content owners simply not knowing where the content is, how many versions there are and what redundant files exist, resulting in duplicative storage use.

That, of course, is a metadata-related issue. But, at some point, this content will be moved from digital tape systems to digital storage systems and ultimately to content creation systems.

These content creation systems take the form of digital nonlinear editing systems (DNLEs), digital audio workstations (DAWs), visual effects systems (VFX), etc. Again, the files are "out in the open," meaning if they were encrypted at rest, they no longer are. How will manufacturers of such content creation and manipulation systems address and maintain the provenance and chain of custody of content? This developing issue will take on increased importance. Further, if we think about the computational aspect of decrypting and manipulating content that resides in an encrypted form, it is a daunting task, especially at higher bit rates and resolutions.

Effective Approaches to Tackle Chain of Custody Challenges in Media Organizations

Ensuring a chain of custody for your content requires a multi-faceted approach, as there is no one-size-fits-all method. Multiple technologies and procedures may be necessary. To start on the right path, begin by diagnosing your specific needs and systematically listing the required solutions. Below, you'll find a range of solutions that can be utilized individually or in tandem.

Digital Rights Management (DRM)	Utilize DRM technologies, including encryption, watermarking and access control mechanisms for permitted access to content and to enforce usage restrictions.
Blockchain	Utilize Blockchain and a distributed public ledger when appropriate for the type of content being addressed. Ensure a tie-in with contract terms (smart contracts).
Content Tracking and Monitoring	Use content tracking and monitoring tools including digital fingerprinting, cryptography, content recognition algorithms and website inspection to detect instances of unauthorized distribution or usage.
Secure Content Distribution	Establish secure distribution systems by using encrypted connections, secure servers and authentication mechanisms to ensure content is only accessed and distributed through authorized networks and subsystems. Implement strong encryption algorithms to safeguard content during storage, transmission and distribution, thus preserving content integrity.
Licensing and Contracts	Establish well-defined licensing agreements and contracts with distributors, partners and content creators outlining permitted uses, distribution rights and limitations to adhere to compliance requirements.
Internal Access Controls	Implement strict access controls, role-based access controls (RBAC), and user authentication and logging mechanisms to limit content access and modification and to track and document content activity. Secure network infrastructure by establishing firewalls, intrusion detection and prevention systems, and virtual private networks (VPNs) to protect content from unauthorized network access and external threats.
Secure Storage	Store content in secure environments, such as encrypted databases or storage systems with access controls, preventing unauthorized copying, modification or theft.
Regular Security Updates and Audits	Ensure the latest security patches and updates are in place for hardware and software. Conduct periodic unscheduled and unannounced security audits to identify vulnerabilities and to be in compliance with industry standards and regulations and to institute procedures for incident response and disaster recovery for content restoration.
Content Metadata and Documentation	It is crucial to establish and preserve content metadata and documentation, including origin, modifications and distribution history, to be used as a reference and evidence of the chain of custody.
Employee Training and Awareness	Employees need to be trained on comprehensive security practices and protocols on a recurring basis.

By implementing these practices and security protocols, media companies can establish a robust chain of custody for their content. These measures protect intellectual property, prevent unauthorized distribution and maintain the trust of audiences and partners.

Crucial Insights into Supply Chain Costs for Media Organizations: Concluding Thoughts

There are, undeniably, costs associated with implementing the various safety nets as outlined above. But consider the lack of chain of custody and the ramifications on global piracy of content. Piracy of film and television content by the third quarter of 2022 was estimated to be at least $29B. If a $200M feature film is leaked before its release, it is critical to be able to describe all of the steps taken to ensure the custody of content and to then best understand what went wrong.

Ensuring the custody of your content is not achieved in one fell swoop by implementing each of the highlighted methods, and you also may not have budgetary approval to do so. What is essential is that you begin to address the two most obvious areas first—access to systems and the logging and tracking of that access.

The cliché in the insurance industry is that you will never know when you need it. But when it comes to content—your Intellectual Property—knowing who originated it and the path it took to the consumer is knowledge that, ultimately, future proofs your revenue streams.

Contact

Edward Hanapole
Managing Director

+1 646 881 9681
ehanapole@alvarezandmarsal.com

Thomas Ohanian
Director

+1 401 935 5410
tohanian@alvarezandmarsal.com

ABOUT ALVAREZ & MARSAL

Companies, investors, and government entities around the world turn to Alvarez & Marsal (A&M) for leadership, action and results. Privately held since its founding in 1983, A&M is a leading global professional services firm that provides advisory, business performance improvement and turnaround management services. When conventional approaches are not enough to create transformation and drive change, clients seek our deep expertise and ability to deliver practical solutions to their unique problems.

With over 8,000 people providing services across six continents, we deliver tangible results for corporates, boards, private equity firms, law firms and government agencies facing complex challenges. Our senior leaders, and their teams, leverage A&M's restructuring heritage to help companies act decisively, catapult growth and accelerate results. We are experienced operators, world-class consultants, former regulators and industry authorities with a shared commitment to telling clients what's really needed for turning change into a strategic business asset, managing risk and unlocking value at every stage of growth.

To learn more, visit: AlvarezandMarsal.com

Follow A&M on: