CAUSATIONCLARITY.COM

SAMPLE EXPERT DEPOSITION REPORT

What an Opposing Expert Report Looks Like When Its Reasoning Is Stress-Tested for Deposition

This is a redacted Expert Deposition Analysis prepared from a publicly filed expert report.

It shows the full adversarial output — not a summary, not a teaser.

5 Analytical Fragility Points	9 Cross-Examination Clusters	4 Concession Pathways
Across reasoning structure, methodology, evidence, and assumption dependencies	Derived directly from the structural gaps in the opinion	Each mapped to the specific admission that matters and how to obtain it

Five Places This Expert Opinion Becomes Vulnerable Under Questioning

Each finding below is documented in the full analysis. The cross-examination questions and concession pathways for each are in Sections 6 and 7.

The Infeasibility Opinion Evaluates the Wrong Problem

The expert's conclusion that checksum-based identification is technically infeasible addresses proactive discovery of unknown files across the full system. It says nothing about reactive blocking of specific checksums already reported to Napster by rights holders. The Metallica submission the expert himself introduces — 470,846 distinct MD5 values covering over two million identified items — is a corpus of precisely known hash values Napster had already received. The opinion forecloses only one of two operationally distinct questions, and it is not the one liability turns on.

Deposition exposure: High.

This concession severs the infeasibility opinion from the knowledge-based liability theory it was designed to defeat.

The Comparator Analogy Omits the Feature That Matters Most for Liability

The report positions Napster alongside cassette decks, VCRs, and CD burners as technologies that enable music sharing. None of those devices maintained a server-side index of what content their users were making available to others in real time. Napster did. The centralized index gave Napster's operators visibility into system contents that no cassette deck manufacturer possessed. The expert acknowledges the architecture but never analyzes what that index means for operator knowledge.

Deposition exposure: High.

The analogy holds at the level of functional output and breaks down at exactly the level where liability analysis operates.

Bot Detection Reveals Filtering Capacity the Infeasibility Defense Denies

The expert defends Napster's real-time behavioral detection and blocking of automated programs as technically sound. That defense concedes the existence of session-level

filtering infrastructure capable of making real-time access decisions. The report does not analyze whether that same architecture could have been applied to flagged users or content. The gap between what the bot-detection discussion acknowledges and what the infeasibility conclusion requires is never resolved.

Deposition exposure: High.

The admission reframes the central question from what Napster technically could not do to what it chose not to do.

The RIAA Causation Argument Has No Record Support Connecting It to Napster

The report argues that the RIAA's engineering failures caused the absence of screening infrastructure Napster would otherwise have used. It cites no document showing Napster evaluated watermarking technology, no evidence that Napster's design decisions were contingent on industry-wide adoption of a marking standard, and no demonstrated link between the RIAA's internal choices and Napster's system architecture. Strip the causation and the section becomes an accurate but legally inert account of the recording industry's internal history.

Deposition exposure: High.

Both causal premises are conceded as unsupported by record evidence.

The Feasibility Determinations Rest on an Undefined Standard

Throughout the technical infeasibility conclusions, the report never states what threshold separates a feasible system from an infeasible one. Imperfection and infeasibility are treated as equivalent without explanation. No benchmark, test, or analytical framework appears in the submitted materials for evaluating that distinction. Without a defined standard, the feasibility conclusions cannot be replicated, tested, or meaningfully challenged on technical grounds. They rest on the expert's judgment, not on any disclosed methodology.

Deposition exposure: High.

Admissibility exposure: Specific Daubert vector on the feasibility conclusions.

WHAT THIS FULL ANALYSIS CONTAINS

The sample below follows the standard seven-section framework used in every Expert Deposition Analysis engagement.

Primary Opinion Target

How the report's central claim is constructed, how the supporting conclusions are layered and sequenced, and where inference is doing work that documented evidence does not perform

Opinion Dependency Points

The unstated assumptions each conclusion depends on, and what happens to the opinion if those premises are examined under oath

Methodological Exposure Points

Where the described methodology fails to visibly produce the conclusions presented, and where credentialed assertion has replaced disclosed derivation

Record Conflict Points

Where the expert's own cited evidence works against the conclusion it purports to support, and where the report's internal characterizations are in tension with each other

Analytical Fragility Points

The five vulnerabilities most exposed under deposition pressure, each assessed for admissibility exposure and evidentiary weight

Cross-Examination Question Sequence

Nine question clusters derived directly from the identified gaps, structured to obtain specific acknowledgments in a defined order

Concession Pathways

Four mapped concessions: the admission target, why it matters, and exactly how the sequence obtains it

The number of fragility points, cross-examination clusters, and concession pathways varies by engagement depending on the expert report, the evidentiary record it relies upon, and the complexity of the opinions being challenged. The admissibility analysis in this sample applies the federal Daubert standard as it would be evaluated in the Northern District of California. Every engagement is assessed under the reliability framework applicable to your jurisdiction and court.

Delivered Within 72 Hours. Fixed Fee. No Consultation Required.

The same framework applied to your expert, your deposition, and your jurisdiction.

Submit your Expert Report for Analysis:

https://causationclarity.com/expert-submit/

FULL SAMPLE – EXPERT DEPOSITION ANALYSIS

This analysis was prepared from the publicly filed expert report of Professor J. D. Tygar, submitted in A&M Records, Inc. et al. v. Napster, Inc. in the United States District Court, Northern District of California in 2000. The source report is public record. The analytical framework applied is identical to what is used in every engagement.

Prepared for: REFERENCE SAMPLE – CAUSATION CLARITY

File Reference: A&M Records, Inc. et al. v. Napster, Inc. — Case No. C 99-5183 MHP

Date of Delivery: September 19, 2024

Expert report Analyzed: Expert Report of J. D. Tygar, dated July 26, 2000

Jurisdiction: Federal. United States District Court, Northern District of California. Daubert Reliability Standard

Prepared by: Raymond Davey Independent Litigation Analyst causationclarity.com
raymond@causationclarity.com

This document is confidential and prepared solely for the use of the receiving attorney. It does not constitute legal advice, medical opinion, or expert testimony.

Note: This is a reference sample prepared in 2026 using a publicly filed expert report from active litigation in 2000. The analytical framework, admissibility standards, and methodology references reflect current practice. Some procedural and legal context may differ from what would have applied at the time of the original filing.

ANALYTICAL REVIEW NOTICE

This document is an independent analytical review of the submitted expert witness report. It is produced by an independent litigation analyst and does not constitute legal advice, technical opinion, or expert testimony. No attorney-client relationship, expert relationship, or professional advisory relationship is created by the preparation or delivery of this document.

The findings, observations, and identified vulnerabilities in this analysis reflect structured adversarial review of the written materials provided. They represent analytical judgment about where weaknesses, contradictions, and evidentiary risks appear to exist based on the submitted report — not conclusions of law, findings of fact, or predictions of litigation outcome. Nothing in this document should be treated as a guarantee, warranty, or assurance about how any argument, motion, deposition, or proceeding will resolve.

The strength of any identified vulnerability depends on facts, documents, and circumstances beyond what was submitted. The analysis is limited to the written record provided. Material not submitted may affect or alter any finding in this document. Where the expert's reasoning is materially dependent on visual exhibits, diagrams, or image comparisons not described in the report text, those elements cannot be analyzed and any affected sections are flagged accordingly. The absence of a flag does not mean the analysis is complete — it means it is complete on the materials received.

This document is intended to inform the professional judgment of the receiving attorney. It is not a substitute for that judgment. The attorney is responsible for independently evaluating every analytical observation before acting on it, for verifying that the identified vulnerabilities hold against the full case record, and for making all strategic decisions independently.

This analysis was prepared using structured analytical methodology applied to the submitted written materials. It reflects the analyst's independent judgment and is not produced, endorsed, or verified by any technical professional, legal professional, or credentialed expert.

EXECUTIVE SUMMARY

This brief provides a structured analysis of the opposing expert's opinion with the specific objective of identifying where the reasoning becomes vulnerable under deposition questioning.

The analysis isolates the opinion's key dependency points and highlights where clarification, concession, or methodological exposure may materially narrow the expert's conclusions.

Key Deposition Vulnerabilities

The infeasibility opinion evaluates the wrong problem.

The expert's conclusion that checksum-based identification is technically infeasible addresses proactive discovery of unknown files across the full system. It does not address reactive blocking of specific checksums already reported to Napster by rights holders. The Metallica submission the expert introduces — 470,846 distinct MD5 values covering over two million identified items — is a corpus of precisely known hash values Napster had already received. The expert's analysis explains why new, unencountered copies evade checksum matching. It is silent on whether Napster could have blocked the values it already held.

Those are operationally distinct questions. The opinion forecloses only one of them.

The comparator analogy omits the feature that matters most for liability.

The report positions Napster alongside cassette decks, VCRs, and CD burners as technologies that enable music sharing. None of those devices maintained a server-side index of what content their users were making available to others in real time. Napster did. That centralized index gave Napster's operators visibility into system contents — a form of visibility no cassette deck manufacturer possessed. The expert acknowledges Napster's architecture but never analyzes what the centralized index means for operator knowledge. The analogy holds at the level of functional output and breaks down at exactly the level where contributory and vicarious liability analysis operates.

Bot detection reveals filtering capacity the infeasibility defense denies.

The expert defends Napster's real-time behavioral detection and blocking of automated programs as technically sound. That defense concedes the existence of session-level

filtering infrastructure capable of making real-time access decisions. The expert distinguishes bot blocking from user blocking on the ground that user identification requires reliable authentication at login, but separately endorses Napster's ID/password system as functional and superior to IP-based identification. The report does not analyze whether Napster's session-level filtering architecture could have been applied to flagged users or content.

The gap between what the bot-detection discussion acknowledges and what the infeasibility conclusion requires remains unresolved.

The RIAA causation argument lacks any record support connecting it to Napster.

Conclusion 6 argues that the RIAA's engineering failures caused the absence of screening infrastructure Napster would otherwise have used. The report cites no document showing Napster evaluated watermarking technology, no evidence that Napster's design decisions were contingent on industry-wide adoption of a marking standard, and no demonstrated link between the RIAA's internal choices and Napster's system architecture. The historical narrative about the RIAA's management failures is detailed and may be accurate. Without the causal premises, it does not bear on what Napster knew or could have done.

The feasibility determinations rest on an undefined standard.

Throughout Conclusions 3 through 5, the expert concludes that various technical approaches are infeasible. The report never states what threshold separates a feasible system from an infeasible one. Imperfection and infeasibility are treated as equivalent without explanation. No benchmark, test, or analytical framework appears anywhere in the submitted materials for evaluating that distinction.

Without a defined standard, the feasibility conclusions cannot be replicated, tested, or meaningfully challenged on technical grounds. They rest on the expert's judgment, not on any disclosed methodology.

Primary Concession Targets

Reactive blocking of already-reported checksums.

The expert must acknowledge that his infeasibility analysis addresses proactive identification of unknown files, not blocking of specific checksum values already

received from rights holders. That concession severs the opinion from the knowledge-based liability theory it was designed to defeat.

Absence of a centralized index in comparator technologies.

The expert must acknowledge that none of his listed comparator technologies maintained a real-time server-side record of what content users were making available. That acknowledgment strips the cassette deck analogy of its capacity to speak to operator knowledge.

Existence of real-time filtering infrastructure.

The expert must acknowledge that bot detection demonstrates session-level filtering capacity within Napster's existing architecture, and that his report does not analyze whether that capacity was applicable to flagged content or users.

Absence of record support for the watermarking causation claim.

The expert must acknowledge he cites no evidence that Napster evaluated watermarking or conditioned its filtering decisions on the RIAA's technical choices. That concession reduces Conclusion 6 from a causation argument to a historical narrative with no demonstrated connection to Napster's conduct.

No defined feasibility threshold.

The expert must acknowledge that his report states no benchmark for distinguishing a technically infeasible system from an imperfect but operable one. That acknowledgment means the feasibility determinations are unreviewable as methodology and rest entirely on his unreplicated judgment.

SECTION 1: PRIMARY OPINION TARGET

The Central Claim

Tygar's report is organized around a single overarching proposition: Napster cannot be held responsible for copyright infringement because it is technically indistinguishable from a broad class of existing, accepted technologies, and because the technical alternatives for preventing infringement are either not feasible or were never made available through failures attributable to the recording industry itself. Every subsidiary conclusion in the report feeds that central proposition. The argument is architecturally defensive: Napster is a neutral conduit, comparable to tools the law has already accommodated, operating in an information environment where no workable rights-identification infrastructure exists.

The report does not advance a single narrow technical claim. It advances a normalized portrait of Napster as a technology that shares structural identity with cassette decks, search engines, FTP clients, and email, embedded inside a broader narrative about the recording industry's failure to create the infrastructure that would make filtering technically possible. Taken together, these interlocking conclusions are designed to deflect both direct infringement arguments and the feasibility of injunctive relief.

The Reasoning Architecture

The report builds its central proposition across three distinct argumentative layers.

Layer One: Normalization of the technology.

The first layer establishes that Napster is not novel. Conclusions 1 and 2 do the work here. Conclusion 1 positions Napster as one of many consumer products that allow users to share recorded music: cassette decks, VCRs, Minidisc recorders, CD burners, ripping software, and portable MP3 players. The implicit argumentative logic draws on the Sony Betamax framework: devices capable of substantial non-infringing use cannot be treated as inherently infringing instruments. Tygar does not cite *Sony v. Universal Studios* explicitly by name in this section, but the structural argument is unmistakable. The list of comparison technologies is extended and granular, including not just general recording devices but dual-dubbing cassette decks and stand-alone CD copiers with disc-at-once functionality. That specificity is deliberate — it positions Napster not as the first

technology capable of facilitating copying, but as the latest in a long, commercially normalized lineage.

Conclusion 2 extends this normalization into the network layer. Napster is placed in a category with email, FTP, the World Wide Web, and search engines including Google, Gnutella, Freenet, and SpinFrenzy. The argumentative function is to characterize Napster's core technical mechanism — peer-to-peer file sharing indexed through a central directory — as a variant of functions foundational to Internet architecture. File sharing, Tygar argues, is not a byproduct of Internet design; it is the design. Treating Napster's file-sharing capability as a basis for liability would logically implicate email and the web itself.

Layer Two: Technical impossibility of compliance.

The second layer addresses what Napster could have done or could be required to do. Conclusions 3, 4, and 5 operate together. Conclusion 3 establishes that Napster has no access to copyright status information and no technically feasible means of acquiring it. Three approaches to identification are considered: file names, checksums, and pre-authorization collection. Each is rejected. File names are unreliable because they are user-generated mnemonics with no standardized correspondence to recording identity. Checksums fail because the same source recording produces different checksums depending on compression settings, mastering differences, analog staging, and encoding software. Pre-authorization is technically infeasible because the scale of the corpus, combined with the impossibility of human review, makes real-time authorization impractical.

Conclusion 4 extends the authorization problem by adding an authentication dimension. Even if rights holders submitted authorizations, Napster would have no cryptographically sound basis for verifying that the submitting party was actually the rights holder. Anyone could falsely represent authorization, and Napster's systems would have no mechanism to distinguish genuine authorization from fraudulent claims.

Conclusion 5 frames the structural consequence of mandatory authorization: it would transform the decentralized architecture of the Internet into a centrally gated permission system, fundamentally incompatible with the Internet's technical design. Tygar presents this as both a technical impossibility and a structural argument about the nature of the medium.

Layer Three: Industry-created conditions.

The third layer is analytically distinctive and carries particular argumentative weight. Conclusion 6 does not merely explain why Napster cannot identify protected content — it assigns responsibility for that condition.

The argument traces the recording industry's efforts to develop rights-marking technology from 1980 forward. The CBS Copycode scheme is described, and its rejection by the government is documented through cited Wall Street Journal reporting. The RIAA's subsequent engagement with Bolt, Beranek, and Newman on watermarking is described in detail, along with that system's rejection by the SDMI in 1999. The SDMI's selection of Musicode as a transitional watermarking standard is presented as evidence that workable technology was available, and had been available for a decade, but was never deployed.

The argumentative conclusion drawn from this history is direct. If the recording industry had made technically sound decisions in the late 1980s or early 1990s, recordings would today carry embedded copyright information. MP3 players and services like Napster could then have screened content by reading that embedded data. The absence of that screening capability is not a failure attributable to Napster. Tygar frames it as a consequence of RIAA's engineering decisions — and presents this not as a neutral historical observation but as a direct rebuttal to any argument that Napster should have been able to identify and filter protected content.

Supporting Conclusions

Conclusions 7, 8, and 9 provide supporting material that reinforces the primary position without advancing it independently.

Conclusion 7 enumerates legitimate uses of Napster involving copyrighted material: space-shifting, format conversion for portable use, distribution by independent artists, academic use, and preview before purchase. The analytical function is to establish that Napster's population of uses is not uniformly infringing and that the system cannot distinguish infringing from non-infringing use even in principle. This reinforces the normalization argument by grounding it in user behavior rather than technical comparison alone.

Conclusion 8 addresses the ID/password authentication system and analyzes it against alternatives including IP-based identification, biometrics, smart cards, public key

certificates, and credit card authentication. The conclusion that ID/password is the most practical available mechanism also serves as a predicate for the argument in Conclusion 9: technical capacity to exclude bots from Napster does not imply a capacity to exclude identified infringers, because the two problems are structurally different. Bots are detectable by behavioral signature during active sessions. Users accused of infringement must be identified at login, which requires reliable authentication — and reliable authentication across the open Internet remains technically unsolved.

Argumentative Pattern

The report follows a recognizable defense-side expert pattern. The structure is layered: establish technological normalcy first, then establish the technical impossibility of the required remedy, then shift causal responsibility for the conditions that created the problem. This sequencing insulates each layer from independent attack. Even if Conclusion 1 were weakened — even if Napster were found distinguishable from cassette decks — Conclusions 3 through 6 would remain intact as independent grounds for the technical infeasibility of filtering. The industry-failure narrative in Conclusion 6 does not depend on the normalization argument in Conclusion 1. Each layer carries independent argumentative weight.

The report also exhibits a characterization strategy common in technology expert work. It consistently frames contested technical claims as matters of consensus or common knowledge within the field. Watermarking technology is described as "well understood" and the subject of undergraduate theses. File sharing is described as fundamental to Internet architecture. ID/password authentication is described as "reasonable and customary." These characterizations do not derive from formal surveys of the field or from cited authority. They derive from Tygar's professional judgment, presented as though they reflect settled technical consensus.

Where the Argument Depends on Inference

Several analytical steps in the report rest on inference rather than demonstrated analysis.

The claim that the same source recording produces categorically different MP3 files depending on encoding parameters is supported by Tygar's description of technical variables and a personal anecdote about multiple pressings of Miles Davis's *Kind of Blue*. The claim is analytically plausible, but the report presents no structured technical

demonstration. The conclusion that RIAA's engineering decisions in the 1980s and 1990s constituted poor engineering rests on Tygar's characterization of news articles and a patent application, not on a formal technical evaluation of the competing proposals. The argument that watermarking would have been technically effective if deployed in the mid-1990s depends on assumptions about adoption rates, hardware standardization, and the robustness of early watermarking systems against attack — none of which the report demonstrates.

These inference points are not contradictions. They are the structural load-bearing elements of the argument — the places where the expert's judgment is doing work that documented evidence does not fully perform. They are identified here as elements of the argument's architecture, not as flaws.

SECTION 2: OPINION DEPENDENCY POINTS

The Technical Infeasibility Conclusion Rests on an Undisclosed Scope Assumption

Conclusion 3 — that Napster cannot distinguish between protected, authorized, and public domain material — is framed as a general technical impossibility. The report presents three potential identification mechanisms (filename matching, checksum comparison, pre-authorization collection), evaluates each, and concludes all three fail. The underlying assumption is never disclosed: that any identification system must work reliably at scale, automatically, in real time, and without human review. The report treats this four-part performance requirement as a given, never stating it explicitly and never defending why each element is necessary before an alternative can be deemed infeasible.

Remove any one of those requirements — allow partial identification, allow probabilistic matching, allow human-assisted review for flagged content — and the infeasibility conclusion weakens structurally.

The report does not show why a partial or imperfect identification system would be legally insufficient. A legal assumption is embedded in a technical argument: that the applicable standard demands complete, automated identification. That assumption is never acknowledged as such.

The Checksum Analysis Assumes Version Proliferation Is Universal and Unmanageable

The report's rejection of checksum-based identification depends on the claim that ripping variations produce unique checksums for every copy of the same recording. The report states this as an observable fact, supports it with the expert's personal experience with Miles Davis and Glenn Gould recordings, and reinforces it with Metallica list data showing 470,846 distinct checksums for a single band's catalog.

The assumption embedded here is that checksum proliferation is extensive enough to make any checksum-based system unworkable for any purpose. The report does not distinguish between high-proliferation scenarios, such as a widely ripped commercial catalog, and lower-proliferation scenarios, such as new releases or catalog recordings distributed predominantly in digital form. It does not analyze whether a checksum

database covering a defined subset of recordings — commercially released, high-volume titles available in controlled digital formats — would still fail. The argument is stated universally, but the evidence it draws on reflects specific conditions.

The Metallica letter data is the report's primary empirical support for checksum failure. Using that data to support a general conclusion about all recordings requires demonstrating that the Metallica scenario represents the broader catalog at issue in this litigation. That inferential step is not visible from the materials provided.

The Filename Analysis Assumes Users Would Systematically Circumvent Any Filter

The report's rejection of filename-based identification relies on two arguments: ambiguity in how files are named, and the likelihood that users would intentionally use misleading or misspelled filenames to evade detection. The second argument depends on an assumption the report treats as demonstrated but does not empirically establish — that evasion would occur at a scale sufficient to render filename filtering useless.

The report cites a website (stopnapster.com) that actively advocates misleading filenames and notes that a search for "Metalica" (misspelled) returned a large number of hits. But the report does not quantify what proportion of files on the Napster network used non-standard naming at the time the report was prepared. The conclusion that systematic circumvention would defeat filename filtering assumes both widespread user awareness of the evasion technique and widespread motivation to employ it. Neither is documented.

The report also assumes that filename filtering would be attempted as a standalone measure rather than as one component of a layered system. Whether filename matching, combined with other signals, could produce actionable results even without perfect accuracy is a question the infeasibility conclusion forecloses without answering.

The Authorization Pre-Check Conclusion Assumes Legal Compliance Requires Prior Authorization

Conclusion 3 states that requiring pre-authorization from rights holders before providing access to material is "technically infeasible and would prevent the effective operation of the utility." The report devotes substantial analysis to why real-time pre-authorization cannot work technically. The embedded assumption — never stated and

never defended — is that any workable authorization system must operate at the moment of each user request, and that post-hoc or batch authorization systems are not legally or operationally viable alternatives.

The report does not consider whether Napster could maintain a list of pre-authorized content indexed against known identifiers and updated periodically rather than queried in real time. It does not consider whether an opt-in mechanism, where rights holders submit authorized content for listing, would satisfy any legal obligation regardless of whether Napster could independently verify claims. The technical infeasibility argument addresses only one model of authorization and assumes that model is the only one legally demanded. That assumption carries significant weight in the conclusion but remains invisible in the report's reasoning.

The Watermarking Conclusion Assumes RIAA's Failures Are Legally Imputable to Napster

Conclusion 6 argues that no widespread watermarking system exists because of poor engineering decisions by the RIAA over two decades. The report traces those failures from Copycode through BBN through the SDMI selection process. The conclusion embedded in this section — made explicit in the final several paragraphs — is that because the RIAA failed to deploy workable watermarking technology, Napster cannot be held responsible for failing to use it.

This conclusion depends on an assumption that is never articulated: that the absence of a deployed industry-wide standard is equivalent to the absence of any available technical measure Napster could have adopted.

The report acknowledges that watermarking technology has existed for a decade, that it has been commercially deployed in image rights management (Digimarc, Playboy), and that the SDMI selected a transitional watermarking technology within three months of its formation. These acknowledgments create internal pressure on the very assumption they are meant to support. The argument asks the reader to accept that because no industry standard emerged, no individual actor could have implemented available technology — that industry-wide adoption was the necessary precondition for any implementation. That logical step is never defended.

The Peer-to-Peer Architecture Argument Assumes Functional Equivalence Establishes Comparable Culpability

Conclusions 1 and 2 rest on an analogical structure: Napster is like cassette decks, like VCRs, like email, like FTP, like search engines. The functional comparison is detailed and extensive. The underlying assumption is that functional similarity to legally sanctioned technologies establishes comparable legal treatment — a legal conclusion imported through a technical argument.

The report does not claim these technologies are identical. It acknowledges that Napster uses a peer-to-peer model distinct from the client-server model of the web. The argument is that the functional output (sharing recorded music) is similar enough that treating Napster differently would be arbitrary. But whether functional similarity at the output level determines legal treatment is not a technical question, and the report never discloses its assumption that it does.

The analogy further depends on treating each listed technology as occupying equivalent legal footing. The VCR comparison imports the Sony Betamax framework without invoking it explicitly. The email and FTP comparisons assume those systems occupy secure legal ground that Napster should share. The report never addresses whether Napster's specific characteristics — centralized index, searchable catalog, named-file download — distinguish it from any of the listed analogues in legally significant ways. Functional overlap is treated as sufficient. The analytical step establishing that sufficiency is not visible from the materials.

The Conclusion That Napster Cannot Know Whether a Use Is Infringing Assumes Ignorance of System-Level Patterns

Conclusion 7 presents a series of hypothetical legitimate use scenarios: the vinyl LP owner, the CD collector using space-shifting, the musician seeking distribution, the student previewing before purchase. These examples demonstrate that Napster cannot know whether any particular file transfer is infringing. The assumption embedded in this reasoning is that the inability to verify individual use purposes means Napster lacks any basis for inference about aggregate use patterns.

The report moves from "Napster cannot know why this user wants this file" to "Napster cannot tell whether a particular use of its system is infringing" without addressing whether system-level evidence — filenames explicitly referencing commercially

released copyrighted works, transfer volume, user account patterns — could support infringement inference even without certainty about individual user intent.

The legitimate use scenarios are deliberately edge cases: the classical music collector, the Aboriginal folk song enthusiast, the academic instructor. The report presents these as illustrations, not frequency estimates. Whether the existence of legitimate use cases renders the overall question of infringing use unanswerable — when legitimate uses may represent a small fraction of actual system traffic — is not addressed.

The ID/Password Conclusion Assumes the Relevant Question Is Identity Verification Rather Than Access Control

Conclusion 8 argues that the ID/password scheme Napster uses is reasonable and superior to alternatives. The analysis compares it against IP address blocking, biometrics, smart cards, public key cryptography, and credit card authentication, finding each alternative inferior. The entire conclusion is constructed within a single frame: the relevant engineering question is how to uniquely and persistently verify user identity.

The report never addresses whether the actual question in this litigation is something different — not how to verify who a user is, but whether Napster's system prevents reinstatement of blocked users or enables rapid re-entry after suspension. The report acknowledges that a blocked user can circumvent the registry-based block by erasing or manually editing the registry, and characterizes this as requiring "a fair level of technical expertise." That characterization is asserted, not measured. The claim that technical sophistication serves as a meaningful barrier to circumvention is unsupported by any data in the report.

The Structural Transformation Argument in Conclusion 5 Assumes a False Dichotomy

Conclusion 5 argues that requiring authorization would transform the web from a decentralized, ground-up information base into a centrally controlled, top-down distribution system. The argument is framed as binary: either the internet operates without authorization requirements, or it becomes a centralized utility. No intermediate model is treated as technically feasible.

The report does not analyze authorization requirements applied selectively to specific content categories, implemented through distributed cryptographic means, or structured through opt-in publisher frameworks. It addresses only a universal pre-authorization requirement applied to every file or web page. The conclusion that structural transformation is inevitable assumes that any authorization requirement, regardless of scope or implementation architecture, produces the described outcome. That assumption is both undisclosed and significant. The entire policy weight of Conclusion 5 depends on it.

SECTION 3: METHODOLOGICAL EXPOSURE POINTS

The foundational problem in this report is not that Tygar lacks credentials. He repeatedly describes a technical landscape, asserts a conclusion that landscape supposedly supports, and then treats the description as the analysis. The gap between description and derivation appears in nearly every conclusion. Where Tygar invokes methodology, he does so to establish general technical context, not to connect that context to the specific system or the specific legal question before the court.

Conclusion 3: The Infeasibility Determination

The report's third conclusion asserts that Napster cannot distinguish between protected and unprotected material, and that requiring pre-authorization is "technically infeasible." This is the report's most consequential technical assertion, and the one with the largest gap between methodology described and conclusion reached.

Tygar identifies three candidate mechanisms for copyright identification: file names, checksums, and a pre-authorization clearance system. He then explains why each is imperfect, and the explanation is accurate as far as it goes. File names are ambiguous. Checksums produce different values for the same source material depending on encoding variables. A human clearance system would be overwhelmed by volume and could be defeated by substitution.

What the report does not show is how evaluating these three mechanisms, and finding each imperfect, produces the conclusion that identification is "technically infeasible." Imperfection and infeasibility are not equivalent conclusions, and Tygar never explains why he treats them as equivalent here. A system that correctly identifies sixty percent of protected files is imperfect. Whether that same system is therefore infeasible for any regulatory purpose is a separate question — one that requires analysis of what accuracy level is needed, for what purpose, under what conditions. The report never establishes what threshold would make a system feasible, never explains how that threshold was determined, and never applies it to the mechanisms under evaluation.

The checksum analysis illustrates this most clearly. Tygar demonstrates, using the Metallica submission data, that a single recording yields a very large number of distinct checksums because of variation in encoding. He is correct that this makes checksum-matching against a static list unreliable. But the report does not evaluate whether a

dynamic checksum database — continuously updated, crowd-sourced, or built by the record labels themselves — would reduce the gap to an acceptable level.

The conclusion that checksums are infeasible rests entirely on the static-list analysis, without establishing that this analysis exhausts the relevant design space.

The file name analysis contains the same structural problem. Tygar demonstrates that file names can be ambiguous, misspelled, or deliberately falsified, and he cites the stopnapster.com site as evidence that users would actively work around name-based filters. But circumvention affects efficacy. Feasibility is a different measure. The report never specifies which is being addressed, and conflates them throughout this section.

Conclusion 4: Authentication Infeasibility

The fourth conclusion holds that Napster has no practicable way to verify that an authorization came from the actual rights holder. The example Tygar uses is a Hotmail account spoofing a Metallica representative's name. His conclusion is that identity verification is not practicable.

The methodology here is a single illustrative failure scenario. The report describes one authentication method — email address verification — demonstrates it is insufficient, and then concludes that authorization checking is not practicable. The analytical step connecting "this one method is insufficient" to "no practicable method exists" is not visible from the submitted materials.

Tygar's own report, later in Conclusion 8, provides an extensive taxonomy of authentication mechanisms: passwords, IP addresses, biometrics, smart cards, public key cryptography, and credit cards. He evaluates each in the context of user identity for access control. He does not apply any of them to the rights-holder authorization problem in Conclusion 4. The report treats the Hotmail scenario as representative of the entire authentication design space without explaining why the same mechanisms evaluated in Conclusion 8 are inapplicable to the authorization context in Conclusion 4. That gap creates significant deposition exposure.

Public key cryptographic certificates — which Tygar describes elsewhere as "an elegant, effective solution to authentication" — receive no evaluation in Conclusion 4 in the context of rights-holder verification. The report does not establish why certificate-based authorization from RIAA, major labels, or a designated licensing authority would fail. Tygar acknowledges in Conclusion 8 that PKI certificates have limitations, primarily

that ordinary users do not commonly hold them. But the authorization question in Conclusion 4 does not involve ordinary users. It involves record labels and their representatives — entities that already operate sophisticated commercial infrastructure.

The report does not address whether PKI-based authorization would be practicable for institutional rights holders.

The conclusion appears to depend on an undisclosed assumption that the authentication burden falls on individual users, but the report never states that assumption or tests it.

Conclusion 6: The RIAA Engineering Assessment

Conclusion 6 argues that watermarking technology was feasible years before the litigation and that RIAA's failure to adopt it earlier reflects poor engineering management. Tygar concludes that had the industry adopted watermarking in the late 1980s or early 1990s, "most recordings would have audio indicators of copyright information which could be used by MP3 players and by Napster software."

The methodology supporting this conclusion is a narrative history of industry attempts at copy protection. Tygar recounts Copycode's failure, the BBN proposal, the SDMI process, and the selection of Musicode as a transitional standard, and then renders the judgment that RIAA used "poor engineering" and that earlier adoption would have been both feasible and effective.

The earliest watermarking work Tygar cites in the audio domain is from a 1993 conference, with Matsui's earlier publications addressing images specifically. Tygar acknowledges that extending image watermarking to audio "would be obvious to someone familiar with digital technology," but that assertion — that the extension would be obvious — is itself a technical conclusion the report never demonstrates. The claim that watermarking was feasible "in the late 1980s or early 1990s" lacks an analytical basis in the submitted materials.

The conclusion that early adoption "would have resulted in a decade's worth of recordings with copyright information clearly marked" compounds this by treating technical availability as equivalent to practical deployment at scale. Whether hardware manufacturers, independent labels, international distributors, and consumer device makers would have implemented an early RIAA standard is not addressed. Tygar notes that SDMI selected a standard "within 3 months of being formed," but does not explain

why the same outcome was not available in 1989. The comparison is asserted, not derived.

There is also an internal tension the report does not resolve. The BBN watermarking system's failure — described as resulting from psychoacoustic compression stripping the watermark — is directly relevant to whether any 1989-era scheme would survive MP3 encoding. Tygar describes the BBN failure and then concludes that an earlier system would have been effective, without establishing why earlier systems would have avoided the compression-stripping vulnerability that defeated BBN.

Conclusion 5: The Architectural Impact Argument

Conclusion 5 asserts that requiring pre-authorization for file sharing would transform the Internet from a decentralized model to a centralized one and would produce severe technical difficulties, possibly preventing the World Wide Web from functioning at all. This is a sweeping conclusion. The methodology behind it is a description of how the web currently operates: decentralized, publisher-initiated, with no central gatekeeper. Tygar then asserts that a pre-authorization requirement would "add delay to publication," "act as an official gatekeeper," and create performance problems that are "almost certainly" severe.

No quantitative or architectural analysis supporting those performance claims appears in the submitted materials. The report does not describe what a pre-authorization system would look like architecturally — whether authorization would require real-time clearance per file request, pre-registration of files, or periodic audit. Without specifying the architecture under evaluation, the claim that it would "almost certainly" produce severe technical difficulties cannot be derived from the analysis described. For a conclusion this broad — that a class of regulatory approaches could prevent the Internet from functioning — the derivation is entirely absent.

Conclusion 9: Bot Detection as Technical Control

Conclusion 9 addresses bots and explains that Napster blocks them for performance reasons. Tygar concludes that this is technically sound and does not contradict Napster's claimed inability to control user identity.

The distinction Tygar draws is coherent on its face: bots are caught in real time while their IP address is known and can be immediately dropped; users who need to be

blocked must be identified at login, where IP addresses are unreliable. But he reaches this conclusion entirely by inference. The report does not describe the specific technical mechanism Napster uses to identify bots — whether it relies on behavioral pattern analysis, request rate thresholds, header inspection, or some other approach. Without describing the mechanism, the report cannot demonstrate that the same mechanism is inapplicable to identifying high-volume infringing users.

A user who downloads thousands of files through Napster in a short period may produce a behavioral signature similar to a bot. The report does not analyze whether Napster's existing detection infrastructure could be adapted to identify that pattern. The conclusion that bot detection and user identification are categorically different technical problems rests on an analogy — the small merchant watching for shoplifters — rather than on technical analysis of Napster's actual detection architecture.

General Methodological Pattern

Across the report, Tygar employs a consistent pattern: describe the technical context in detail, cite supporting evidence from industry publications and news articles, and then state the conclusion. The derivation connecting the evidence to the conclusion is replaced by assertion. This pattern is most visible in the feasibility conclusions but appears throughout.

The report discloses no methodology for evaluating feasibility as a technical concept. There is no stated standard for what makes a technical requirement feasible rather than infeasible, no threshold, no test, no comparison set. When Tygar concludes that something is infeasible, that conclusion rests on identifying practical difficulties, not on applying a defined analytical framework that would allow another analyst to replicate the evaluation and reach the same result.

Under Daubert, the absence of a testable methodology is the critical exposure point. An expert who describes technical facts accurately but does not disclose how those facts produce the conclusions presented leaves the derivation entirely within the expert's unreviewable judgment. That is not a methodology. It is credentialed assertion.

SECTION 4: RECORD CONFLICT POINTS

The Metallica Checksum Evidence Works Against the Conclusion It Purports to Support

Conclusion 3 argues that Napster cannot identify copyrighted files because checksum-based identification is technically infeasible. Different encoding choices produce different checksums for the same underlying recording, meaning a single Metallica track could yield thousands of distinct hash values. The expert uses the Metallica letters to demonstrate this: Howard King's 18 May letter identified 2,280,474 items with 470,846 distinct MD5 checksums, a number the expert calls "clearly far larger than the number of recordings Metallica actually has issued."

That framing converts the evidence into an argument for infeasibility. The same evidence cuts the other direction.

The existence of 470,846 distinct checksums presupposes that Napster's system captured and retained enough file-level data to allow that enumeration. King's letter was not speculative — it listed specific files with specific hash values derived from Napster's own system. If Napster had no access to file-level information, the checksum list could not have been generated from Napster data at all. The report treats the size of the checksum list as evidence of infeasibility while simultaneously relying on that list's existence as proof that checksum data was present in the system. That tension is never resolved.

The inference the expert draws — that the sheer volume of checksums makes identification impractical — does not follow automatically from 470,846 distinct values. The report does not establish how many unique Metallica recordings exist in commercial release, so the ratio cannot be evaluated. Without that baseline, the conclusion that the checksum count exceeds what Metallica "actually has issued" is asserted rather than derived. If Metallica has released several hundred tracks across studio albums, live releases, and bootlegged concert recordings explicitly acknowledged in King's letter as non-infringing, the ratio between tracks and checksums becomes the operative question. The report never calculates it.

The "Chris Isaak" Observation Undermines the Expert's Own Reliability, Not Just Metallica's

The report notes that two items in Metallica's "Top 100 Distinct Digital Recordings" list appear to be songs by Chris Isaak, using this to suggest that Metallica's identification methodology was unreliable. The observation is framed as an internal critique of the opposing party's evidence.

The problem is what the expert then does with it. Having identified that files on the Metallica list were mislabeled or misattributed, the report simultaneously maintains that file names are an unreliable basis for identification — a point used earlier in Conclusion 3 to argue that Napster cannot screen copyrighted material. These two arguments depend on the same underlying premise in contradictory ways. When it serves the argument against filtering feasibility, mislabeled files prove that file names are useless identifiers. When it serves a critique of Metallica's methodology, mislabeled files prove that Metallica did a poor job.

The report cannot deploy file name unreliability as evidence of the futility of filtering and then deploy a specific mislabeled file as meaningful evidence of evidentiary failure in the opposing party's submission — unless the expert is claiming that the mislabeling is observable and meaningful, which cuts against the earlier claim that file names convey no reliable information.

The report also acknowledges that some files on the Metallica top 100 list are live recordings and notes that King's letter explicitly disclaimed copyright infringement as to fan-made concert recordings. The expert frames this as raising questions about whether those files should have appeared on the list. But the expert does not establish that the live recording files were fan-made rather than professionally produced concert releases. The ambiguity the expert identifies as a problem for Metallica's list is precisely the same ambiguity the expert elsewhere says Napster has no way to resolve. Using that ambiguity to impugn the opposing party's evidence while simultaneously using it to excuse Napster's inability to filter creates an internal consistency problem the report never addresses.

The RIAA Engineering History Undermines the Stated Conclusion About Current Technical Feasibility

Conclusion 6 argues that the RIAA's history of poor technical decisions left the industry without a viable watermarking standard, meaning Napster has no marking infrastructure to rely on for identifying protected recordings. That framing positions the record industry's delay as the operative cause of the current absence of workable screening technology.

The historical account the expert provides to support that conclusion contains specific admissions that work against it.

The report states that the SDMI, within three months of being formed, "was able to collect a large number of excellent technical proposals for realizing marking of copyright information." This characterization is the expert's own. If the SDMI — formed in early 1999 — could assemble viable proposals within three months, the technical challenge is described as solvable and recently solved, not inherently intractable. The expert then argues that if the RIAA had applied similar engineering management in the late 1980s, "most recordings would have audio indicators of copyright information which could be used by MP3 players and by Napster software." That sentence explicitly acknowledges that watermarking technology was mature enough by the late 1980s or early 1990s to have been implemented, and that its implementation would have made screening "easy to technically effect."

The expert draws from this history the conclusion that the RIAA's past failures explain the current absence of screening infrastructure. But the internal logic of the report instead establishes that the technology was available well before it was adopted, that non-adoption reflected a management failure rather than a technical impossibility, and that once properly managed, viable proposals emerged quickly. The expert's own account of the SDMI's three-month success shifts the argument from "this cannot be done" to "this was not done on time due to poor decisions." Those are structurally different claims, and the second does not support a conclusion that Napster faces a technically insurmountable screening problem. It supports the conclusion that the infrastructure deficit is remediable.

The report also notes that Musicode was designated as a "transitional technology" and that copy protection information "using Musicode can be included in recordings starting now." This statement appears in the section establishing that watermarking is currently

available. The expert does not reconcile this with the broader claim in Conclusion 3 that Napster has no way to identify protected recordings. Musicode's designation as a working transitional standard, capable of being included in recordings at the time of the report's writing, sits in tension with the claim that no widespread rights-marking technology exists. The expert's own evidence supports the proposition that a functional standard was selected and was deployable — just not yet universally adopted.

The Dual-Dubbing and Consumer Device Analysis Introduces Evidence That Cuts Against the Sony Standard Defense

Conclusion 1 builds an analogy between Napster and consumer recording technologies — cassette decks, VCRs, Minidisc recorders — to argue that Napster occupies the same legal and technical space as products previously found to have substantial non-infringing uses. The comparative list is extensive, and the expert draws on personal experience with consumer equipment to populate it.

Within that section, the expert acknowledges that the Serial Copy Management System (SCMS) in Minidisc and DAT equipment "purportedly prevents multigenerational copying of source material." He then immediately describes three methods for defeating SCMS, including use of a professional dual-dubbing unit available "for prices as low as about $2000" and a circuit that "a person with some electronics training can easily build," with plans "fully available on the Internet." The stated purpose is to show that SCMS protection is technically easy to defeat.

This material supports the expert's analogy only if bypassing copy protection qualifies as normal, widely practiced consumer behavior.

Presenting SCMS circumvention as practical and accessible means the comparison class the expert is constructing — technologies that permit music sharing — now includes technologies that specifically defeat rights management protections built into the medium. The report does not separate the analogy based on lawful consumer use from the analogy based on circumvention-enabled use. The expert presents SCMS defeat methods without qualification as to their legality and without acknowledging that the example potentially introduces a different legal context than simple home recording. This internal framing issue requires no external source to surface — it appears within a single extended passage in the same section.

The Adaptec Easy CD Creator reference presents a related problem. The expert quotes the product's warning notice in full, including its explicit statement that the product "MAY BE DESIGNED TO ASSIST YOU IN REPRODUCING MATERIALS IN WHICH YOU OWN THE COPYRIGHT OR HAVE OBTAINED PERMISSION TO COPY FROM THE COPYRIGHT OWNER." He presents this warning as evidence that commercial software enables music copying. But the product's own language expressly conditions lawful use on copyright ownership or permission, and the expert treats that condition as irrelevant to the comparative analysis. Including a product whose manufacturer explicitly disclaimed unauthorized copying as a comparator for Napster, without distinguishing how that disclaimer affects the analogy, leaves the cited evidence in tension with the conclusion it is meant to support.

The Section 512 Analysis Rests on a Legal Characterization the Expert Is Not Positioned to Make

The report's Conclusion 2 contains a paragraph beginning: "Based on my lay reading of section 512(a) of Title 17, I believe that Napster qualifies for an exemption for liability and relief for infringement under the terms of that section." The expert lists five conditions and asserts Napster meets each.

The expert expressly frames this as a "lay reading," which is an unusual self-characterization for an expert opinion offered in a legal proceeding. More significantly, one of the five conditions he identifies is that "Napster does not screen the material but provides connection and routing information automatically." The expert asserts this as a factual characterization of Napster's operation. Conclusion 9 of the same report describes how Napster actively detects and rejects bots — specifically, that "Napster similarly bans bots from accessing the search engine functions of Napster." The basis for that rejection involves Napster-side detection of automated behavior patterns, which is a form of real-time screening.

Whether automated program rejection qualifies as "screening" under Section 512(a) is a legal question the expert is not addressing in a legal capacity. But the factual predicate — that Napster does not screen material — is directly complicated by the expert's own description of bot detection in Conclusion 9. The two sections address the same factual point and the characterizations are not reconciled. The expert treats the absence of content screening and the presence of behavioral screening as categorically distinct

without explaining why that distinction holds under the statutory language he is purporting to apply.

The HP Computer Citation Introduces Promotional Marketing Language as Technical Evidence

The expert quotes at length from Circuit City's website describing the HP Pavilion 8670C as "Your Personal Music Machine" and a device enabling users to "make your own customized audio CDs by pulling songs straight from the Internet." This is advertising copy, not a technical specification. At the level of marketing intent, it does establish that consumer PCs were designed and sold with music copying as an expected use.

The problem is that the expert cites this material to support a conclusion about the widespread commercial availability of CD-copying technology, implicitly positioning it as industry recognition of that functionality as a normal product use. Advertising copy from a consumer electronics retailer does not establish technical equivalence between CD-burning functionality and Napster's peer-to-peer file sharing network. The expert never draws an explicit functional equivalence between pulling songs from the Internet via a PC's built-in CD-writer software and Napster's indexed, search-driven peer-to-peer architecture. The technology described in the HP advertisement operates through a client-server model, which the expert elsewhere specifically identifies as architecturally distinct from Napster's peer-to-peer model. The analogy depends on a functional equivalence the report never demonstrates, and the source material whose absence makes that gap visible is not an external authority — it is the expert's own architectural distinction, stated elsewhere in the same report.

SECTION 5: ANALYTICAL FRAGILITY POINTS

Fragility Point 1: The Technological Infeasibility Opinion Depends on a Scope the Expert Defined Himself

Concession target: The expert would have to acknowledge that his conclusion — that filtering or authorization is "technically infeasible" — rests on requiring Napster to screen all content across the entire system, rather than applying targeted filtering to identified infringing files.

Where the vulnerability appears: Conclusion 3 states that Napster "can not distinguish between" protected, permitted, and unprotected material, and that requiring pre-authorization "would prevent the effective operation of the utility." The expert reaches this conclusion by working through three potential filtering mechanisms — filename matching, checksum comparison, and pre-authorization — and demonstrating why each fails at scale. The argument is built around comprehensive, system-wide filtering as the operative assumption.

Why the concession matters: The expert never addresses the narrower question of whether Napster could have implemented targeted filtering of specific, already-identified infringing files that had been reported to it. The Metallica example the expert himself introduces — 470,846 distinct checksums across 2,280,474 items — demonstrates that Napster had received a substantial corpus of specifically identified content with corresponding checksums. The infeasibility argument is structured around proactive, exhaustive identification. But the plaintiff-side liability theory does not require Napster to have identified all infringing content. It requires Napster to have acted on what it knew.

If the expert concedes that checksum blocking of previously reported, specifically identified files was technically feasible — even if imperfect — the infeasibility opinion loses its force as a defense to knowledge-based liability.

The expert's own checksum discussion acknowledges that MD5 checksums were submitted to Napster. He then argues against their utility by noting that encoding variation produces different checksums for the same underlying recording. But that argument cuts only against Napster proactively finding new copies, not against Napster blocking the specific checksums it had already received. The expert never addresses the narrower scenario, and that gap is where the opinion is most exposed.

Admissibility exposure or evidentiary weight: This is an evidentiary weight issue, not an admissibility issue. The opinion clears the Daubert threshold. But the concession would substantially narrow the operative scope of the infeasibility argument and deprive it of its force at the infringing-knowledge stage of the liability analysis.

Fragility Point 2: The Comparator Technologies Argument Depends on an Equivalence the Report Does Not Establish

Concession target: The expert would have to acknowledge that none of the consumer technologies he identifies as comparators — cassette decks, VCRs, ripping software, CD burners — maintained a centralized index of every file its users were making available to every other user simultaneously, in real time.

Where the vulnerability appears: Conclusion 1 constructs a comparator list spanning roughly a dozen consumer technologies and argues that Napster "allows users to share music" in the same functional tradition as all of them. The expert explicitly states that "the fundamental idea of sharing music is not new" and that "[s]pecialized consumer equipment facilitating sharing of musical recording has been popular long before Napster came on the scene." This structural equivalence between Napster and prior consumer devices carries significant weight in the report's overall architecture — Conclusions 3, 4, and 7 all depend on Napster being positioned as merely one node in a long line of passive, general-purpose tools.

Why the concession matters: None of the comparators on the expert's list maintained a centralized index. A cassette deck does not know what recordings its users are copying. A VCR does not maintain a server-side directory of every recording every user has designated for sharing. Ripping software operates locally and is invisible to any network operator. Napster operated a central server that actively catalogued the shared libraries of its users and matched them to requesters.

The expert acknowledges this architectural distinction in Conclusion 2 when he contrasts the client-server model of the World Wide Web with Napster's peer-to-peer model — but uses it only to argue that Napster is not unique in offering peer-to-peer functionality. He does not address what the centralized index means for Napster's actual knowledge of its system's contents.

The comparator argument breaks down at the point where it matters most for contributory and vicarious liability: what the operator knew, when, and whether it had the technical ability to act on that knowledge.

If the expert concedes under oath that none of his listed comparators maintained a real-time, server-side index of what content users were making available, the analogy to a cassette deck — the most rhetorically powerful element of the comparator argument — is revealed to omit the feature most relevant to liability.

Admissibility exposure or evidentiary weight: Evidentiary weight primarily. The comparator methodology is not so flawed as to warrant exclusion. But the concession materially weakens the moral and legal equivalence the report works hardest to establish.

Fragility Point 3: The RIAA Failure Argument Shifts Responsibility Without Establishing Causation

Concession target: The expert would have to acknowledge that even if the RIAA had successfully deployed watermarking technology in the 1980s or 1990s, nothing in the watermarking framework would have obligated Napster to implement screening, and nothing in the report establishes that Napster actually conditioned its filtering decisions on the availability of such technology.

Where the vulnerability appears: Conclusion 6 is the longest and most technically detailed section in the report. It traces the RIAA's history of failed copy-protection efforts from Copycode through BBN's watermarking proposal to SDMI, characterizing the RIAA's technical record as one of "poor engineering" and "engineering bungles." The expert closes by arguing that if the RIAA had adopted a marking scheme in the late 1980s, "most recordings would have audio indicators of copyright information which could be used by MP3 players and by Napster software."

Why the concession matters: The argument functions to shift responsibility for the absence of technical filtering from Napster to the RIAA. Two premises carry that shift, and the report demonstrates neither.

First, it assumes that Napster would have implemented watermark-based screening if the technology had been available. The report contains no evidence that Napster evaluated watermarking technology, considered implementing it, or made any documented decision about it in either direction. The expert's opinion on what Napster

"would" have done is inferential and unsupported by any material in the submitted record. Second, it assumes a causal chain — that the RIAA's failure caused the absence of screening — without establishing that Napster's filtering decisions were contingent on the RIAA's technical choices. These are independent actors, and the report documents no link between them on this question.

Under deposition, the expert would have to acknowledge that he has no basis in the record for either premise. That concession reduces Conclusion 6 from a causation argument to a historical narrative about the RIAA's internal failures — technically detailed, but without a connection to the operative liability question of what Napster knew or could have done with the tools available to it.

Admissibility exposure or evidentiary weight: This fragility point carries a marginal admissibility dimension. The causal claim embedded in Conclusion 6 — that the RIAA's failures caused Napster's inability to screen — resembles the kind of opinion that requires a disclosed analytical methodology for the causation finding. The report describes no such methodology. Under Daubert, a causal conclusion presented without explanation of the analytical steps used to reach it faces a potential reliability challenge. More immediately, once the causal premises are severed, Conclusion 6 has no load-bearing function in the liability analysis.

Fragility Point 4: The Bot-Detection Argument Concedes Technical Capability That Undermines the Infeasibility Defense

Concession target: The expert would have to acknowledge that Napster successfully distinguished and blocked automated programs in real time, using behavioral pattern recognition, while simultaneously claiming that it could not identify and block known infringing users or content.

Where the vulnerability appears: Conclusion 9 explains that Napster blocked bots for performance reasons and that this is "a perfectly sound reason." The expert then attempts to distinguish bot-blocking from user-blocking by arguing that bots are caught "in the act" while user-blocking must occur at login and depends on reliable identification. He offers the analogy of a small-merchant shoplifter to support that distinction.

Why the concession matters: The expert's own account of the bot-blocking mechanism establishes that Napster was capable of implementing dynamic, real-time filtering logic

— distinguishing between acceptable and unacceptable access and acting on that distinction in the moment. He defends this capability as technically sound. The distinction he draws between bot-blocking and user-blocking is narrower than he acknowledges. The bot-blocking mechanism identifies behavioral signatures and terminates sessions. That same real-time, session-level access gives Napster the technical foothold to act on filename content, IP patterns, and user-account flags at the moment of a search request or download initiation.

The argument that users can evade identification through dynamic IP addresses and registry workarounds is a circumvention argument, not an infeasibility argument. And in Conclusion 8, the expert concedes that Napster's ID/password scheme is functional and superior to IP-based identification. If Napster can reliably identify users for purposes of granting access — which the expert affirms — the claim that it cannot reliably identify them for purposes of blocking creates a structural tension the report does not resolve.

Under oath, the expert would have to concede either that bot-blocking demonstrates real-time filtering capacity, or that the ID/password mechanism he defends as reliable is not in fact reliable enough to support blocking.

Either path shifts the operative question from what Napster technically could not do to what Napster chose not to do.

Admissibility exposure or evidentiary weight: Evidentiary weight. The internal tension does not render the opinion unreliable as a methodological matter. But the concession reframes the central question from technical capacity to operational choice — a framing that serves the plaintiff's theory of knowing facilitation rather than the defense's theory of structural impossibility.

SECTION 6: CROSS-EXAMINATION QUESTION SEQUENCE

The following deposition questions are derived directly from the identified methodology gaps, assumption dependencies, contradictions, and fragility points in this expert report.

Cluster 1: Targeted Blocking of Reported Checksums [FRAGILITY]

Establishes that the infeasibility opinion addresses proactive identification of unknown files, not reactive blocking of specifically reported checksums already received by Napster.

1. Your report states that Howard King's May 18 letter to Napster identified 2,280,474 items with 470,846 distinct MD5 checksums, correct?
2. Each of those 470,846 checksums is a specific value that could be compared against a file presented to Napster's system, correct?
3. Your report's infeasibility analysis for checksum matching addresses whether Napster could proactively identify new, previously unknown files, correct?
4. Your report does not separately analyze whether Napster could have blocked the specific checksums it had already received in King's letter, correct?

Cluster 2: The Centralized Index and the Comparator Technologies [FRAGILITY]

Forces acknowledgment that none of the expert's listed comparator technologies maintained a server-side, real-time index of what content all users were simultaneously making available.

1. Your report identifies cassette decks, VCRs, Minidisc recorders, and CD burners as technologies that similarly allow users to share music, correct?
2. A cassette deck does not maintain any record of what recordings its users are copying, correct?
3. A VCR does not maintain a server-side directory of recordings its users have designated for sharing with other users, correct?

4. Napster operated a central server that catalogued the shared libraries of its users and matched them to requesters in real time, correct?
5. Your report does not analyze what that centralized index means for what Napster knew about the contents of its system at any given moment, correct?

Cluster 3: Bot Detection and Real-Time Filtering Capacity [FRAGILITY]

Forces acknowledgment that Napster implemented real-time behavioral filtering to block automated programs while the report simultaneously claims it lacked the technical capacity to act on known infringing content.

1. Your report states that Napster bans bots from accessing its search engine functions, correct?
2. That ban operates in real time — Napster identifies and terminates a bot session while it is occurring, correct?
3. Your report describes that bot identification as "a perfectly sound reason" for the filtering Napster applies, correct?
4. Your report also states that Napster's ID/password scheme is functional and superior to IP-address-based identification for recognizing users, correct?
5. Your report does not analyze whether Napster's existing real-time session-level filtering infrastructure could be applied to block flagged users or flagged filenames at the point of a search request, correct?

Cluster 4: The Infeasibility Standard Is Never Defined [ADMISSIBILITY]

Establishes that the report contains no stated threshold, test, or analytical framework for distinguishing a technically infeasible system from an imperfect but operable one.

1. Your report concludes that checksum-based identification is "technically infeasible," correct?
2. Your report demonstrates that checksum matching is imperfect because encoding variation produces different checksums for the same underlying recording, correct?

3. Your report does not state what accuracy level a checksum-matching system would need to achieve before it would qualify as feasible, correct?
4. Your report does not define any threshold, benchmark, or test for distinguishing a technically infeasible system from a technically imperfect one, correct?

Cluster 5: PKI Authorization and the Authentication Design Space [ADMISSIBILITY]

Forces acknowledgment that the report's authentication infeasibility conclusion is built from a single failure scenario and does not evaluate the authentication mechanisms the expert himself identifies elsewhere in the same report as available.

1. Your report concludes in Conclusion 4 that Napster has no practicable way to verify that an authorization came from the actual rights holder, correct?
2. The example your report uses to reach that conclusion is the inability to verify whether an email came from an authorized Metallica representative, correct?
3. Your report in Conclusion 8 describes public key cryptographic certificates as "an elegant, effective solution to authentication," correct?
4. The authorization question in Conclusion 4 involves record labels and their representatives, not individual consumers, correct?
5. Your report does not analyze whether PKI-based authorization would be practicable for institutional rights holders such as major record labels, correct?

Cluster 6: The Checksum Count and the Missing Baseline [SECONDARY]

Establishes that the report's primary empirical argument for checksum infeasibility — 470,846 distinct checksums for Metallica — cannot be evaluated without a baseline of how many distinct Metallica recordings actually exist in commercial release.

1. Your report states that 470,846 distinct MD5 checksums for Metallica's catalog is "clearly far larger than the number of recordings Metallica actually has issued," correct?
2. Your report does not state the number of distinct Metallica recordings in commercial release, correct?

3. Your report does not calculate the ratio between distinct commercial recordings and the checksums identified in King's letter, correct?

4. Your report does not analyze whether the checksum count changes materially if the comparison is limited to commercially released studio recordings rather than the full catalog, correct?

Cluster 7: The Watermarking Causation Gap [FRAGILITY]

Forces acknowledgment that the report contains no evidence that Napster evaluated watermarking technology, and no analytical basis for the claim that the RIAA's failures caused Napster's absence of screening infrastructure.

1. Your report concludes that if the RIAA had adopted watermarking in the late 1980s, Napster "could" have used those audio indicators to screen recordings, correct?

2. Your report does not cite any document, communication, or record showing that Napster evaluated watermarking technology at any point, correct?

3. Your report does not cite any evidence that Napster's filtering decisions were contingent on the availability of an industry-wide watermarking standard, correct?

4. Your report does not analyze what Napster actually considered or rejected when deciding what content controls to implement, correct?

Cluster 8: SCMS Circumvention and the Comparator Class

Establishes that the expert's comparator analysis incorporates technologies specifically in their circumvention-enabled configuration, without acknowledging that the comparison class has shifted from lawful consumer use.

1. Your report identifies Minidisc and DAT recorders as comparator technologies alongside Napster, correct?

2. Your report acknowledges that those devices incorporate Serial Copy Management System protection that "purportedly prevents multigenerational copying," correct?

3. Your report then describes three methods for defeating SCMS, including a dual-dubbing unit available for approximately $2,000 and a circuit buildable by someone with basic electronics training, correct?
4. Your report does not distinguish between the lawful consumer use of those devices and their use after SCMS has been deliberately defeated, correct?

Cluster 9: Section 512 Screening Condition and Bot Detection

Forces acknowledgment that the expert's factual predicate for the Section 512 safe harbor — that Napster does not screen material — is directly contradicted by his own description of Napster's bot-detection operations in the same report.

1. Your report states that one condition for Napster qualifying under Section 512(a) is that "Napster does not screen the material," correct?
2. That statement appears in Conclusion 2, correct?
3. Your report in Conclusion 9 states that Napster detects and bans bots from accessing its search engine functions, correct?
4. That ban requires Napster to identify behavioral characteristics of the accessing program in real time, correct?
5. Your report does not reconcile the statement that Napster does not screen material with the description of Napster's active bot-detection and rejection process, correct?

SECTION 7: CONCESSION PATHWAYS

Pathway 1: The Infeasibility Opinion Addresses the Wrong Question

The Admission Target

The expert would have to acknowledge under oath that his technical infeasibility analysis evaluates whether Napster could have proactively identified unknown infringing files across the entire system, and that he conducted no separate analysis of whether Napster could have blocked the specific checksums it had already received in identified form from rights holders.

Why the Admission Matters

This admission severs the infeasibility opinion from the liability theory it was designed to defeat. The expert built Conclusion 3 around a universal screening problem: can Napster distinguish protected from unprotected material at scale, in real time, automatically, across an open network? The answer to that question may well be no. But that is not the question liability turns on at the knowledge stage. The plaintiff's theory does not require Napster to have discovered infringement on its own. It requires Napster to have acted on specific infringement it had been told about.

The Metallica letter data the expert himself introduces — 470,846 distinct checksums covering 2,280,474 identified items — is a corpus of precisely known, specifically enumerated hash values that Napster received and held. The expert's checksum analysis explains why new, unknown copies of a recording will generate different checksums that Napster cannot predict or proactively find. It says nothing about whether Napster could have blocked the checksums it was already given. Those are different operations. One is discovery; the other is execution.

The infeasibility argument runs against discovery and is then silently imported to defeat execution.

Once the expert is pinned to that distinction under oath, the opinion no longer covers Napster's failure to act on reported content. The infeasibility defense shrinks to a residual argument about new files, while the knowledge-based liability window — acting on what Napster knew — remains fully open.

How the Admission Is Obtained

The questioning begins by establishing the expert's own factual predicate: the Metallica checksum data, its volume, and what it represents. The expert cannot retreat from those numbers — he put them in the report to support his argument. Once he confirms that each checksum is a specific value capable of being compared against any file in the system, the sequence narrows to a single gap: whether the report addresses reactive blocking of those reported values separately from proactive identification of new ones. The report does not make that distinction. The expert cannot answer yes without contradicting the text. The admission that the analysis does not address reactive blocking of already-reported checksums follows structurally. No technical expertise is needed to see the gap once the expert has confirmed what the analysis does and does not include.

Pathway 2: The Centralized Index Undermines the Comparator Analogy Where It Matters

The Admission Target

The expert would have to acknowledge that none of the consumer technologies he identifies as functional comparators — cassette decks, VCRs, CD burners, ripping software — maintained a server-side, real-time index cataloguing what content every user was simultaneously making available to every other user on the network.

Why the Admission Matters

The comparator argument is structurally load-bearing. Conclusions 3, 4, and 7 all benefit from positioning Napster as one node in a long tradition of passive, general-purpose technologies. The cassette deck analogy is the report's rhetorical anchor: if sharing music via Napster is legally and technically equivalent to sharing music via a cassette deck, then Napster's operator knowledge and capacity to act are no more culpable than a cassette deck manufacturer's. That equivalence is what the comparator list is designed to establish.

The centralized index breaks the analogy precisely where contributory and vicarious liability analysis operates. A cassette deck's manufacturer has no visibility into what any user is copying at any given moment. Napster's central server does. It actively catalogued shared libraries, matched them to requesters, and maintained those records in real time. The expert's own report acknowledges this architecture in Conclusion 2,

but deploys it only to distinguish Napster from the World Wide Web — not to address what the centralized index means for operator knowledge.

Once the expert concedes that none of his comparators maintained a real-time server-side inventory of user-shared content, the analogy no longer holds where it needs to hold. The comparator technologies tell us nothing about what Napster's operators knew about system contents, because those technologies generated no operator-accessible knowledge. Napster's centralized index did.

The equivalence the report works hardest to establish becomes analytically unstable at exactly the liability-relevant feature the analogies omit.

How the Admission Is Obtained

The sequence works by establishing each comparator on the expert's own terms before isolating what the comparators lack. The questioning walks through the listed technologies one at a time — not to dispute that they enable music sharing, but to confirm that each operates locally, without any server-side record of what its users are copying or sharing. The expert will confirm this readily; it is simply true, and the report does not claim otherwise. Once the full comparator list is confirmed as maintaining no centralized index, the architectural fact about Napster's central server is introduced using the expert's own language from Conclusion 2. The expert cannot deny that Napster maintained a centralized index. The final question — whether the report analyzes what that index means for Napster's knowledge of system contents — surfaces the gap the expert left open. He did not analyze it, and acknowledging that under oath materially weakens the comparator argument's capacity to speak to the knowledge question.

Pathway 3: Bot Detection Converts the Infeasibility Defense into a Choice Defense

The Admission Target

The expert would have to acknowledge that Napster implemented real-time behavioral filtering to detect and block automated programs, and that his report does not analyze whether that same real-time, session-level infrastructure could have been applied to block flagged users or flagged filenames at the point of a search request or download initiation.

Why the Admission Matters

This admission reframes the central question of the entire technical report. The report's governing structure is technical incapacity: Napster could not have done what plaintiffs say it should have done. Bot detection creates a significant analytical vulnerability in that structure. Napster's system identified behavioral signatures, made real-time judgments about whether access should be permitted, and terminated sessions on that basis. The expert calls this "a perfectly sound reason" for filtering. He is right that it is technically sound — and that is precisely the problem for the infeasibility defense. A system that can make real-time access decisions based on behavioral pattern recognition is not a system that lacks the technical architecture for filtering. It is a system that chose what to filter.

The expert's attempt to distinguish bot detection from user blocking depends on arguments about dynamic IP addresses and registry workarounds — circumvention arguments, not incapacity arguments. The expert also defends Napster's ID/password scheme as functional and superior to IP-based identification for recognizing users. If that scheme reliably identifies users for access — which the expert affirms — the claim that it cannot reliably identify them for blocking requires an explanation the report does not provide.

Once the expert concedes that bot detection demonstrates real-time filtering capacity at the session level, the residual infeasibility arguments reduce to the question of circumvention by determined users. Circumvention is an efficacy argument, not a feasibility argument.

The shift from "cannot do it" to "could not prevent all circumvention" substantially narrows what the expert's opinion actually establishes — the opinion no longer forecloses the plaintiff's theory, but argues about how perfectly the controls would have worked.

How the Admission Is Obtained

The questioning anchors to the expert's own description of bot detection and his own characterization of it as technically sound. The expert will confirm both, because the report endorses bot detection explicitly. The sequence then draws out the technical specifics: bot detection operates at the session level, in real time, based on behavioral pattern recognition. The expert confirms this too. The critical question — whether the report analyzes whether that same session-level infrastructure could be applied to

flagged users or filenames — requires only that the expert account for what his report contains. It does not address that question. He will have to say so.

The admission that his report does not analyze whether Napster's existing real-time filtering capacity was applicable to content or user blocking lands cleanly, because it is a factual question about what analysis the report undertook. Nothing in the bot-detection section addresses the adjacent filtering question, and the expert cannot fabricate an analysis that does not appear in the submitted materials.

Pathway 4: The RIAA Causation Argument Has No Record Support

The Admission Target

The expert would have to acknowledge that he identifies no document, communication, or record showing that Napster evaluated watermarking technology, and no evidence that Napster's filtering decisions were contingent in any way on the availability of an industry-wide watermarking standard.

Why the Admission Matters

Conclusion 6 functions as a responsibility-shifting argument: the RIAA's engineering failures caused the absence of the screening infrastructure that Napster would otherwise have been able to use. Strip the causation, and Conclusion 6 is an accurate but legally inert account of the record industry's internal technical history — detailed, perhaps useful for context, but disconnected from anything Napster did or decided.

Two independent premises carry the causal argument. First, that Napster would have used watermark-based screening if the technology had been available. Second, that the RIAA's failures prevented that technology from being available to Napster. The record the expert cites supports neither premise. He identifies no evidence that Napster ever evaluated watermarking, considered it, or decided against it for any reason. Without that foundation, the claim about what Napster would have done is speculation. The second premise — that the RIAA's choices caused Napster's absence of screening — requires a demonstrated link between two independent actors' decisions that the report does not establish.

Once both premises are conceded as unsupported by record evidence, Conclusion 6 loses its causal function entirely. What remains is a history of the RIAA's management

failures — technically detailed, but bearing no demonstrated relationship to what Napster knew, what tools were available to it, or what it chose not to do.

How the Admission Is Obtained

The questioning moves directly from what the conclusion claims to what the report cites. The expert's conclusion about what Napster "could" or "would" have done had watermarking been available is stated in his own words in the report. The sequence then asks the expert to identify, in the submitted materials, any document showing that Napster evaluated watermarking, any evidence that Napster conditioned its filtering decisions on the RIAA's technical choices, and any analysis connecting the RIAA's failures causally to Napster's system design. None of that appears in the report. The expert cannot identify evidence that is not there.

Each acknowledgment that the record does not support a specific premise is an incremental concession. The cumulative effect is to establish that the causal structure of Conclusion 6 rests entirely on inference drawn from historical narrative. An expert who cannot point to record support for either causal premise, when directly asked, has effectively confirmed that the conclusion is asserted rather than derived.

GET THIS TYPE OF ANALYSIS FOR YOUR FILE

This example was produced from a single publicly filed expert report.

The analytical framework remains consistent across engagements, while the analysis itself becomes specific to your expert, your case theory, your jurisdiction, and the evidentiary record the expert relies upon.

Expert Deposition Analysis is designed for the moment after expert reports are exchanged and before deposition preparation begins — when understanding exactly where the opposing opinion becomes vulnerable matters most.

Each engagement is delivered within 72 hours of confirmed submission and is provided at a fixed fee. No consultation call is required.

If you would like the same structured analysis applied to your file, you can submit the expert report and relevant materials below.

https://causationclarity.com/expert-submit/