

ION Video Ltd (ASX:IOV)

Freedom to Operate Clears Path for New Patent

Melbourne, Australia, 17 March 2026: ION Video Limited (ASX: IOV) ("ION" or "the Company") advises that it has received an independent Freedom to Operate patent search and analysis from Alder IP Pty Ltd, confirming that ION's Tokenised Virtual Video Delivery System and Method can be commercialised in key jurisdictions with low identified infringement risk when implemented as described in the Company's provisional filings.

Highlights

- Independent Freedom to Operate search completed by Alder IP in the United States, Europe, Australia and at the international PCT level, focused on the Tokenised Virtual Video Delivery System and Method.
- No existing granted patent was identified that claims the integrated virtualisation engine, AI orchestration layer, tokenised governance and secure resolution architecture described in ION's Claim 1; all key prior art examples were assessed as low or, at worst, manageable risk.
- The analysis confirms that the Netflix, Sandpiper, Ericsson and other cited patents address traditional streaming or authentication problems and do not cover ION's programmable video assembly, cryptographic video token, hardware-attested resolution or content wallet model.
- Taken together with Alder IP's earlier novelty and inventive-step opinion, the Freedom to Operate work provides ION with a coherent legal position: the new patent is both patentable and capable of being deployed commercially without infringing the closest known prior art, when implemented as disclosed.
- This assessment supports ION's strategy to license its infrastructure globally and underpins ongoing partner discussions and technical validation work.

Background: Tokenised Virtual Video System

ION's Tokenised Virtual Video Delivery System and Method is designed to solve the problem of how intelligent systems can assemble, govern and monetise video in real time without exposing raw media or duplicating files.

At the core of the invention is a shift from file-based video to reference-based virtual video:

- A virtualisation engine converts rendered video files into metadata-only reference containers, retaining ISO Base Media File Format structures while removing media sample data.
- An AI orchestration layer then modifies the sequencing instructions inside these containers to assemble personalised streams, without ever touching the underlying media samples.
- A token issuance service generates cryptographic video tokens that bind consent, licensing, transaction logic and micro-payment instructions to each resolution event.
- A secure resolution service, operating inside a hardware-attested trusted execution environment, dereferences authorised segments from remote sources only when a valid token is presented, logging each dereference event to an auditable transaction layer.
- A playback environment acts as a content wallet, holding multiple tokens from independent content owners, dynamically assembling streams in real time and terminating playback instantly if consent is revoked.

This architecture is intended to support the emerging agentic AI era, in which autonomous systems assemble and deliver video on behalf of users and institutions and need a way to enforce rights, consent and commerce at the moment video is resolved.

Alder IP Freedom to Operate Search

Alder IP conducted a Freedom to Operate search for ION covering patent applications and granted patents in:

- The United States
- Europe
- Australia
- PCT applications (WIPO)

The search drew on multiple databases, including Patseer, Patentscope, USPTO, Espacenet, Free Patents Online, AusPat and Google Patents, and was anchored on Claim 1 of ION's provisional specification for Tokenised Virtual Video Delivery System and Method.

Freedom to Operate work is different from novelty searching. Novelty analysis asks whether an invention is new and inventive compared to existing disclosures, which underpins the ability to obtain a patent. Freedom to Operate asks a different question: whether making, using or selling the invention would infringe someone else's existing, in-force patents in a target market.

In this case, Alder IP's mandate was to identify patents that might limit ION's ability to deploy its tokenised Virtual Video system commercially in those jurisdictions.

Summary of Key Findings

Alder IP's analysis confirms that, while there are patents dealing with aspects of video streaming, authentication and secure delivery, none claim the same combination of features described in ION's Claim 1.

The report highlights three main prior art families as the closest references:

1. A Netflix patent relating to improving start-up times of streaming media by pre-fetching metadata and licences.
2. A Sandpiper CDN patent focused on user authentication inside a content delivery network.
3. An Ericsson patent dealing with secure over-the-top live video delivery using conventional licence and encryption workflows.

In each case, Alder IP concluded that:

- The cited patents address traditional streaming or authorisation problems, not programmable virtual video assembly.
- None disclose a virtualisation engine that removes media samples while preserving ISO structures, combined with an AI orchestration layer that resequences content without accessing raw media.
- None describe a cryptographic video token acting as an integrated authorisation gatekeeper that binds licensing, consent and micro-payments to individual segment resolution events.
- None teach a secure resolution service restricted to a hardware-attested trusted execution environment that logs every dereference to an auditable transaction layer, or a playback environment functioning as a multi-owner content wallet.

On that basis, Alder IP assessed the potential infringement risk associated with the closest identified patents as low, provided that ION implements its system in line with the architectural features described in its own filings.

The report also notes that some patents have already expired or will expire within standard terms, and that expired rights revert to the public domain.

Combined Position with Novelty Opinion

On March 10, 2026, ION announced that Alder IP's novelty search and legal opinion had confirmed that the Tokenised Virtual Video Delivery System and Method meets the tests of novelty and inventive step when assessed against prior art from organisations including Ericsson, Wells Fargo, Snap, AT&T, Genetec and PayPal, across multiple major patent offices.

That work established that ION's integrated architecture, combining virtualisation, AI-driven sequencing, consent-governed delivery and micro-payment settlement at the moment of resolution, is not anticipated by existing disclosures and is therefore patentable.

The latest Freedom to Operate analysis complements this by addressing the separate question of commercial deployability. Taken together, the two opinions provide ION with:

- Independent confirmation that its new system is both patentable and differentiated.
- An external view that, in the target jurisdictions, there is no single existing patent that would prevent ION from launching its tokenised Virtual Video infrastructure, when implemented as described.
- A more detailed understanding of where older streaming and authentication patents begin and end, and where ION's claims sit outside that prior art.

This combined legal footing is important as ION moves from describing its architecture to integrating it with partners and commercial platforms.

Strategic Implications for ION

The Company views this Freedom to Operate outcome as a significant de-risking step for its tokenised Virtual Video strategy. It supports ION's plans to:

- Progress from provisional filings to PCT and national phase applications with greater confidence in the commercial usability of the invention.



- Engage with hyperscalers, chip providers, video platforms, agentic AI companies and enterprise partners on pilots and licensing discussions grounded in independent legal analysis.
- Position its tokenised Virtual Video system not only as a patentable idea, but as a deployable infrastructure layer for AI and agentic video experiences in the United States, Europe, Australia and beyond.

As previously communicated, Finbar O'Hanlon and AJ Palmer are planning a global roadshow across the United States, Europe and the Asia-Pacific region to meet key decision makers, supported by ION's work with Canaccord Genuity and its ongoing programme of technical validation and commercial engagement.

Further updates on patent prosecution, partner activity and commercial milestones will be provided as material developments occur in line with the Company's continuous disclosure obligations.

Yours Sincerely

Anthony Baker

Chief Executive Officer and Director

View the link to the original ASX Announcement: [Here](#)

Ion Video Pty Ltd
Level 2, 161 Collins St,
Melbourne 3000, Victoria

Alder IP Ref: 42282

Attention: Anthony Baker

March 16, 2026

Re: Patent “Freedom to Operate” search for ION Video Pty Ltd relating to “Tokenised Virtual Video Delivery System and Method”

Dear Anthony,

We have completed our Freedom to Operate patent search relating to **Tokenised Virtual Video Delivery System and Method** as described in the provisional specification filed and the documents shared.

A. SCOPE

A Freedom to Operate Search is a search performed to determine whether a specific product, process, can be commercially launched without infringing on existing, in-force patents held by others.

The primary objective is to determine if the production, sale, or use of the invention infringes upon any existing patent claims. If the Applicant (company) has the freedom to operate within its industry without facing any legal consequences.

The FTO search was conducted using different databases, such as Patseer, Patentscope, USPTO, ESPACENET, Free Patents Online, AusPat and Google Patents to extract relevant references.

The search covered the below jurisdictions:

- USA
- Europe
- Australia and
- WIPO

For the US database, the search was for patent applications granted and/or published in the US in the last 25 years; while for the WIPO database, the search was in the last 31 months.

Please note that patents filed outside of the aforementioned jurisdictions would not have been detected. Additionally, only patents filed at least 18 months prior to this search would have been detected by the search as it generally takes 18 months for the patent offices to publish the specifications.

For infringement to occur, the alleged infringer must be shown to have used the claimed invention for a commercial purpose within the protected jurisdiction during the life of the patent. The alleged infringing product must take or use each and every feature of at least one claim of a granted patent to infringe.

Pending patent applications cannot be technically infringed until they have been examined, found valid and then subsequently been granted. Pending applications identified in the report were not extensively reviewed by Alder IP as the claims and scope of pending patent applications is usually restricted during patent examination processes.

Additionally, it is possible, under special circumstances in USA, to request reissuance or re-examination to vary the claims of granted patents and these instances would not have been detected by this FTO Search.

Please note that expired patents are open to public access and freely available to be used without license or approval of the owner.

In USA, the maximum term may be extended wherein the owner has informed the Patent Office of delays caused by clinical trials (these extensions may be up to 5 years) and also US Patent Office awards automatic extensions to maximum term for time lost during the examiner's consideration and evaluations.

We note that whilst all possible care is taken when compiling this report, some patents may not have been taken that were incorrectly coded or entered by the relevant patent offices and we are not responsible for errors in the Patent Offices databases.

B. KEY FEATURES

In conducting the search, we used Claim 1 defining the essential features of the invention:

Claim 1 :

A system for programmable video assembly, comprising:

- **a virtualization engine, wherein the engine is configured to convert a rendered video file into a reference container by extracting metadata and removing media sample data;**
 - wherein the virtual video container retains ISO Base Media File Format box structures while being devoid of media sample data.
 - wherein the step of resolving referenced media data involves issuing MDAT range requests to the remote media data sources.
 - further comprising an artificial intelligence orchestration layer configured to modify the sequencing instructions of the reference container without accessing raw media samples.
- **a token issuance service, wherein the service configured to generate a cryptographic video token binding transaction, consent, and licensing information;**
 - wherein the token issuance service includes a unique session nonce in each generated token to prevent unauthorized resolution reuse.
 - wherein the transaction metadata includes instructions for micro payments triggered by individual segment resolution events
 - wherein the cryptographic video token may function as an integrated authorization gatekeeper that operates independently of the media payload by excluding media sample data and direct file paths, enforces the right to resolve by providing the necessary cryptographic permissions and binds governance logic to the resolution event.

- **a secure resolution service, wherein the service dereferences remote media data upon successful validation of the cryptographic video token; further comprising logging each individual media dereference event to an auditable transaction layer.**
 - wherein the secure resolution service is restricted to operating within a hardware-attested trusted execution environment.
 - wherein the logged dereference events trigger a commercial action selected from a group consisting of billing, royalty allocation, and advertising insertion.
- **a playback environment, wherein the playback environment stores multiple tokens and dynamically assembling video streams in real-time from authorized references.**
 - wherein the playback environment is configured to manage independent tokens from multiple content owners within a single session wherein the playback environment may function as a content wallet capable of managing multiple tokens from independent content owners.
 - wherein the system is configured to terminate the video stream instantly upon the revocation of user consent parameters associated with the token.

C. SUMMARY OF KEY IDENTIFIED PATENTS

Assignee/ Applicant	Patent/ Publication No.	Title	Expected Expiry Date	Potential Risk of Infringe- ment	Comment
Netflix Inc	EP 2791847 B1	Improving startup times of streaming digital media playback	12/12/2032	Low	<p>This patent primarily relates to techniques for improving the startup time of streaming digital media by retrieving metadata and pre-processing license requests prior to a user initiating playback of a selected media title.</p> <p>The focus of the cited technology is on reducing playback latency and accelerating the initiation of streaming through early metadata retrieval and license acquisition.</p> <p>However, the cited document does not teach or suggest an AI orchestration layer capable of modifying sequencing instructions without accessing raw media samples, a cryptographic video token system that binds licensing, consent, and transaction information, or secure media dereferencing.</p>
Sandpiper Cdn LLC	US 8,595,778 B2	User authentication in a content delivery network	29-05-2032	Low	<p>The cited document focuses on the method of authorizing delivery</p> <p>The present invention is not authorizing a stream its validating a resolution event for a virtualized asset.</p> <p>The cited document relies on a Subscription Database to determine rights.</p> <p>However, the present invention uses a cryptographic video token that is an "integrated authorization gatekeeper." this token is not just a "yes/no" flag; it is a programmable object.</p>
Ericsson AB	US 12,244,881 B2	Secure over-the- top live video delivery	25/10/2042	Low	<p>The cited document describes a traditional secure delivery workflow.</p> <p>The present invention is a virtualized delivery system where the "video" being delivered is actually a set of instructions (metadata) resolving to remote sources in real-time.</p> <p>The claims of the cited document are restricted to the management of encryption keys and license server delivery.</p> <p>They do not encompass the programmable assembly of video or the use of hardware-attested trusted execution environments for dereferencing events.</p>

A more detailed summary of the full list of identified patents is attached as **Annexure A** and this list includes extracts of the independent claims. The above summary is focused on the key patents of interest that were detected and focused on the closest examples of the prior art in our opinion.

We also note that we have assumed that all patent and patent applications identified in this search were valid and that no assessment of novelty or inventiveness of each identified patent has taken place.

D. CONCLUSION

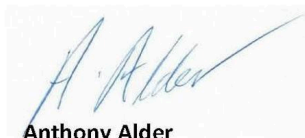
Based on the above analysis, Alder IP believes that ION Video product does not reasonably infringe any of the reviewed patents provided that the risk mitigation advice has been accepted and implemented for the relevant jurisdictions.

Please refer to **Annexure A** for a detailed summary of all patents reviewed.

This report and the analysis within are intended solely for the purpose of providing a opinion regarding the product. This interpretation is based on publicly available information from various sources and should not be construed as a formal legal opinion.

The findings are for the internal use and no part of this report shall be publicly distributed, published, or offered for sale without the explicit permission. This report is intended to serve as a risk assessment tool, it does not constitute a guarantee of definitive legal clearance for commercialization.

Yours faithfully



Anthony Alder

NSW Supreme Court Solicitor/Patent Attorney
Btech (Biotech) LLB MIP FIPTA



MEMBER OF
THE LAW SOCIETY
OF NEW SOUTH WALES



CorporateINTL
GLOBAL AWARDS
WINNER 2016

CorporateINTL
GLOBAL AWARDS
WINNER 2017

CorporateINTL
GLOBAL AWARDS
WINNER 2018

Encl. Annexure A – Detailed Summary
Annexure B – FTO Raw Data Report



Annexure A

Assignee/ Applicant	Patent/Publication No.	Title	Expected Expiry Date	Claim discussion	Proposed Risk Mitigation
Netflix Inc	EP2791847 B1	Improving startup times of streaming digital media playback	12/12/2032	<p>Claim 1</p> <p>A computer-implemented method (300) for a client device to obtain authorization to stream a requested media title, the method comprising: outputting, for display in a user interface (400), a plurality of media titles available for streaming playback;</p> <p>prior to receiving a user request (308) to begin streaming playback of any of the plurality of media titles, retrieving, by operation of one or more computer processors, metadata (306, 510) associated with at least a first one of the plurality of media titles;</p> <p>upon receiving the request to play the first media title (520), generating, based at least in part on the metadata, a request for a license (310) authorizing playback of the first media title; and</p> <p>upon receiving the license (312, 540) for the first media title, beginning streaming playback (318, 550) of the first media title.</p> <p>Claim 10</p> <p>A system, comprising:</p> <p>one or more computer processors; and</p> <p>a memory (230), wherein the system is configured to perform an operation for obtaining authorization to stream a requested media title, the operation comprising:</p> <p>outputting, for display in a user interface (400), a plurality of media titles available for streaming playback;</p> <p>prior to receiving a user request (308) to begin streaming playback of any of the plurality of media titles, retrieving, metadata (306, 510) associated with at least a first one of the plurality of media titles;</p>	<p>Differentiate by structural necessity.</p> <p>Netflix pre-fetches for speed; your engine converts the file into a reference container devoid of media samples.</p> <p>Avoid describing metadata extraction as a latency-reduction tool.</p> <p>Ensure the claim emphasizes that the container is non-functional without MDAT range requests.</p>

Sandpiper Cdn LLC	US 8,595,778 B2	User authentication in a content delivery network	29-05-2032	<p>upon receiving the request (306, 520) to play the first media title, generating, based at least in part on the metadata data, a request for a license (310) authorizing playback of the first media title; and upon receiving the license for the first media title (312, 540), beginning streaming playback (318, 550) of the first media title.</p> <p>Claim 1</p> <p>A computer-implemented method for authorizing delivery of a video stream to an end user, wherein the video stream is associated with a content publisher, the method comprising:</p> <p>receiving a request from the end user for delivery of the video stream to the end user across a network;</p> <p>querying a subscription database associated with the content publisher, in response, processing a reply from the subscription database to determine whether the end user has authorization to receive delivery of the video stream;</p> <p>and</p> <p>performing at least one of:</p> <p>transmitting a notification to the end user indicating that the end user is not authorized to receive delivery of the video stream based on the processing of the reply from the subscription database; and</p> <p>initiating delivery of the video stream to the end user based on the processing of the reply from the subscription database, wherein the reply from the subscription database indicates the end user is authorized to receive delivery of the video stream.</p>	<p>Contrast the authorization logic.</p> <p>Sandpiper relies on a static database lookup.</p> <p>The present invention uses cryptographic tokens with session nonces bound to individual segment resolution events.</p> <p>Avoid using simple "Yes/No" subscription gates.</p> <p>Emphasize micro-payments triggered by specific resolution events.</p>
Microsoft Technology Licensing LLC	US 10,455,286 B2	Protected media decoding system supporting metadata	08/03/2039	<p>1. A method implemented in a computing device, the method comprising:</p> <p>obtaining video content from a media source, the video content including metadata as well as protected video content;</p> <p>extracting the metadata from the video content to obtain extracted metadata, the extracting the metadata including removing the metadata from the video content;</p> <p>providing the extracted metadata to a video decoder without providing the video content to the video decoder for processing by the video decoder;</p> <p>providing the video content with the metadata removed from the extracting to a secure digital rights management component;</p>	<p>Focus on the AI orchestration.</p> <p>Microsoft separates data for secure decoding paths.</p> <p>Avoid defining the system as a "secure decoding pipeline."</p> <p>Instead emphasize the AI layer that modifies sequencing instructions of the reference</p>

Liability limited by a scheme approved under Professional Standards Legislation.

				<p>receiving, from the secure digital rights management component, a re-encrypted version of the video content, the re-encrypted version of the video content comprising a version of the video content from which the protected video content has been decrypted and re-encrypted based on a key of the computing device;</p> <p>providing the re-encrypted version of the video content to the video decoder for decoding of the re-encrypted version of the video content to yield decoded video content rather than decoding of the video content including metadata; and</p> <p>providing the extracted metadata and the decoded video content to an application for playback.</p> <p>7. A method implemented in a computing device, the method comprising:</p> <p>obtaining video content from a media source, the video content including metadata as well as protected video content;</p> <p>extracting the metadata from the video content to obtain extracted metadata, the extracting the metadata including removing the metadata from the video content;</p> <p>providing the extracted metadata to a video decoder without providing the video content to the video decoder for processing by the video decoder;</p> <p>providing the video content with the metadata removed from the extracting to a secure digital rights management component, the secure digital rights management component decrypting the protected video content and providing decrypted video content to a secure decoder component for decoding of the decrypted video content to yield decoded video content rather than decoding of the video content including metadata; and</p> <p>providing the extracted metadata and the decoded video content to an application for playback.</p> <p>13. A computing device comprising:</p> <p>a media source component configured to obtain video content from a media source, the video content including metadata as well as protected video content;</p> <p>an extraction component configured to extract the metadata from the video content to obtain extracted metadata, extracting the metadata</p>	<p>container without accessing raw samples.</p>
--	--	--	--	---	---

Liability limited by a scheme approved under Professional Standards Legislation.

Intel Corp .	EP 2832102 B1	Methods and systems for cryptographic access control of video Images (11)	31-03-2032	<p>including removing the metadata from the video content, and provide the extracted metadata to a video decoder without providing the video content to the video decoder for processing by the video decoder; a secure digital rights management component configured to receive the video content with the metadata removed from the extracting and provide the protected video content to the video decoder for decoding of the protected video content to yield decoded video content rather than decoding of the video content including metadata; and a video decoder component configured to provide the extracted metadata and the decoded video content to an application for playback.</p> <p>1. A method of cryptographic access control - CAC - of video, comprising:</p> <ul style="list-style-type: none"> - by a metadata generator (225), generating (1215) metadata, said metadata representing an access control policy - ACP - associated with the video, the ACP including authorization rules and cryptographic information associated with an encryption policy; - by an encryptor (220), encrypting (1220) the video into an encrypted video (230) according to said encryption policy; and - by an encoder (240), encoding (1225) said encrypted video (230) into an encoded video (130) with said authorization rules and said cryptographic information, said encoded video having multiple segments; <p>wherein the authorization rules and cryptographic information are intended for decrypting and rendering the encoded video; characterized in that said encoding includes encoding different time segments of the encrypted video with corresponding different authorization rules, wherein the authorization rules take into account user specific access controls, including Motion Picture - MP - ratings, an MP rating being embedded in a predetermined segment of said encoded video (130), each segment including a different rating intended for a different type of users.</p>	<p>Emphasize payload independence.</p> <p>Intel embeds rules in the media.</p> <p>The token in the present invention functions independently of the media payload.</p> <p>Avoid storing permissions or ratings inside media segments.</p> <p>Instead restrict all resolution to a hardware-attested TEE..</p>
Comcast Cable Communications LLC	US 11,792,458 B2	Managing concurrent content playback	13/7/2042	<p>1. A method comprising:</p> <ul style="list-style-type: none"> receiving, by a user device and from a content server, an indication of a permission granting the user device access to a content asset; sending, by the user device and to the content server, a request for a segment of the content asset; and receiving, by the user device, from the content server, and based on a determination by the content server that the number of permissions currently granted to the user device exceeds the number of desired 	<p>Highlight the "Content Waller".</p> <p>Comcast manages limits for a single asset.</p>

Ericsson AB	US 12,244,881 B2	Secure over-the-top live video delivery	25/10/20242	<p>1. A method for managing secure distribution of audio or video content comprising: generating a series of content encryption keys for encrypting a single audio or video content item, each content encryption key associated with a different portion of the single audio or video content item wherein client devices requesting the single audio or video content item is further provided with key expiration information usable by the client devices to identify transitions between portions of the single audio or video content item that use different ones of the content encryption keys; and</p>	<p>Focus on real-time consent Ericsson uses key expiration. Avoid relying on standard key rotation for security. Rather, focus on instant termination upon revocation of</p>
				<p>15. A computer-readable medium storing instructions that, when executed, cause: receiving, by a user device and from a content server, an indication of a permission granting the user device access to a content asset; sending, by the user device and to the content server, a request for a segment of the content asset; and receiving, by the user device, from the content server, and based on a determination by the content server that the number of permissions currently granted to the user device exceeds the number of desired concurrent communication sessions by the user device, an indication that access to the another segment of the content asset has been denied.</p>	
				<p>8. An apparatus comprising: one or more processors; and memory storing instructions that, when executed by the one or more processors, cause the apparatus to: receive, by a user device and from a content server, an indication of a permission granting the user device access to a content asset; send, by the user device and to the content server, a request for a segment of the content asset; receive, by the user device, from the content server, and based on a determination by the content server that the number of permissions currently granted to the user device exceeds the number of desired concurrent communication sessions by the user device, an indication that access to the another segment of the content asset has been denied.</p>	<p>Avoid using simple concurrency/limit-counting logic. Rather, focus on managing independent tokens from multiple content owners within a single session.</p>

			<p>11. A computerized device operable as a workflow manager for managing secure distribution of audio or video content, comprising memory operative to store computer program instructions; one or more processors; input/output interface circuitry; and interconnect circuitry coupling the memory, processors and input/output interface circuitry together, wherein the processors are operative to execute the computer program instructions from the memory to cause the computerized device to: generate a series of content encryption keys for encrypting a single audio or video content item, each content encryption key associated with a different portion of the single audio or video content item wherein client devices requesting the single audio or video content item is further provided with key expiration information usable by the client devices to identify transitions between portions of the single audio or video content item that use different ones of the content encryption keys; and provide the content encryption keys to a license server for delivery to the client devices for use in decrypting the content item, the license server being operative to establish that a requesting client device is authorized to access the content item, the license server being further operative to securely deliver the content encryption keys to a requesting client device whose authorization to access the content item has been established.</p>	<p>user consent parameters bound to the token.</p>
--	--	--	--	--



ENDS

Authorised for release by the Board of Directors

For more information, please contact:

ION Enquiries:

- Anthony Baker - Chief Executive Officer
- Email: investor.relations@ion.video
- Tel: +61 3 8672 7186

Media & PR Enquiries:

- Rod North - Managing Director, Bourse Communications
- Email: rod@boursecommunications.com.au
- Tel: +61 3 9510 8309 or +61 408 670 706

About ION Video Limited

ION Video Limited (ASX: IOV) is an infrastructure company that has developed patented technology to virtualise video at the file architecture level, transforming static files into programmable data. Protected by four foundational patents, ION's technology enables intelligent systems to access and compose with existing video content as programmable data, without transcoding.

For additional information about ION, please visit www.ion.video

Forward-Looking Statements

This announcement contains forward-looking statements regarding ION's technology, market positioning and strategic priorities. These statements are based on current expectations and are subject to risks and uncertainties. Actual results may differ materially from those expressed or implied in these statements. This announcement has been prepared in compliance with ASX Listing Rule 3.1 regarding continuous disclosure obligations.

ION Video Limited (ASX: IOV) ACN 149 796 332