

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Google LLC,
Petitioner,

v.

Ericsson AB
Patent Owner.

Case IPR2025-00003
Patent No. 9,313,178

**DECLARATION OF JOHN VILLASENOR, Ph.D. IN SUPPORT OF
PATENT OWNER'S RESPONSE**

TABLE OF CONTENTS

I.	Introduction	1
A.	Background and qualifications	1
B.	Engagement	5
C.	Materials considered	5
II.	Relevant legal standards	6
A.	Person of ordinary skill in the art	6
B.	Burden of proof	8
C.	Claim construction	8
D.	Obviousness	8
III.	The '178 Patent	10
IV.	The Petition does not meet “parsing content information from the playback request response, the content information including content encryption keys. . .” as recited in all claims	14
A.	Relevant claim language	14
B.	The Petition’s theory	15
C.	Peterka’s teachings contradict and refute the Petition’s theory	16
V.	The Petition does not meet “parsing content information from the playback request response, the content information including . . . content encryption <i>key identifiers</i> ” as recited in all claims	45
A.	Relevant claim language	45
B.	The Petition’s theories	46
C.	Peterka’s message sequence numbers or timestamps are not “content encryption <i>key identifiers</i> ”	47

D.	The Petition fails to demonstrate obviousness with respect to “content encryption key identifiers”	49
VI.	The Petition’s theory based on Peterka’s expiration times and pull embodiment does not meet “detecting content encryption key rotation boundaries”	52
VII.	The Petition’s theory based on Peterka’s notifications does not meet the “issuing requests” requirement of all challenged claims	62
VIII.	Conclusion	66

I, John Villasenor, Ph.D., do hereby declare as follows:

I. Introduction

A. Background and qualifications

1. I received a B.S. in electrical engineering from the University of Virginia in 1985, an M.S. in electrical engineering from Stanford University in 1986, and a Ph.D. in electrical engineering from Stanford University in 1989.

2. Between 1990 and 1992, I worked for the Jet Propulsion Laboratory in Pasadena, CA, where I helped to develop techniques for imaging and mapping the earth from space. Since 1992, I have been on the faculty of the Electrical Engineering Department of the University of California, Los Angeles (UCLA). Between 1992 and 1996, I was an Assistant Professor; between 1996 and 1998, an Associate Professor; and since 1998, I have been a full Professor. For several years starting in the late 1990s, I served as the Vice Chair of the Electrical Engineering Department at UCLA. In addition to my faculty appointment in the UCLA Samueli School of Engineering, I hold faculty appointments in (and have taught classes in) the Department of Public Policy within the UCLA Luskin School of Public Affairs, in the UCLA School of Law, and in the UCLA Anderson School of Management.

3. In the UCLA Samueli School of Engineering, I have taught courses on information processing and communications, addressing systems, algorithms, networks, and devices. I have created and taught many courses during my time at

UCLA. Among other courses, I have taught communications at UCLA, including consideration of delivery of content across wired and wireless networks, as well as the associated protocols.

4. In addition to my teaching, at UCLA I have performed extensive research over the past several decades on devices, communications, and networks, and their use in content acquisition, processing, and secure communication. This research has considered topics including methods to acquire and process information, and the design of devices, networks and protocols used in relation wireless and wired communications of data, and methods for ensuring content is secured, and accessible only to those who have a right to access it. My work has addressed hardware, algorithms, networking, and protocols for reliably, efficiently, and securely communicating information in the presence of constraints on delay, bandwidth, complexity, and power; and hardware, algorithms, protocols.

5. In relation to these and other topics, my research has addressed software, algorithms, hardware, networking, security, rights management, protocols and other aspects of systems and devices relating to acquiring, processing, storing, communicating, and presenting digitally-represented information. My work has addressed both the hardware and software aspects of systems, and has included consideration of factors such as bandwidth utilization, data rate, protocols,

interaction with users including mechanisms for validating users, and mechanisms for user input and output, including interfaces and the associated software and circuitry.

6. I am an inventor on approximately 20 issued and pending U.S. patents in areas including signal (including image and video) processing, data compression, communications, and cybersecurity. I have published over 175 articles in peer-reviewed journals and academic conference proceedings. I have also been asked on multiple occasions to provide congressional testimony on technology topics, including the associated legal and policy implications.

7. In addition to my work at UCLA, I am a nonresident senior fellow at the Brookings Institution in Washington, D.C. Through Brookings I have examined a wide range of topics at the technology/policy intersection including cybersecurity, the integrity of the electronics supply chain, wireless mobile devices and systems, and artificial intelligence.

8. In addition to publishing in traditional academic venues such as engineering journals, engineering conference proceedings, and law reviews, I have published papers through the Brookings Institution and articles and commentary in broader-interest venues including Billboard, the Chronicle of Higher Education, Fast

Company, Forbes, the Los Angeles Times, the New York Times, Scientific American, Slate, and the Washington Post.

9. I have also served as a senior fellow at the Hoover Institution at Stanford and an affiliate of the Center for International Security and Cooperation (CISAC) at Stanford. In relation to those affiliations, I led a research project funded by the U.S. Department of Homeland Security aimed at improving cybersecurity in U.S. critical infrastructure. I am also a member of the Council on Foreign Relations.

10. I have several decades of experience in early-stage technology venture capital in the San Francisco Bay Area. In that capacity I have met with a large number of startup companies seeking venture financing spanning a wide range of technology areas, including those listed above. Among other things, I have helped to evaluate the proposed technology, the competitive landscape, the market opportunities and risk, the strength of the team, and the company's IP strategy and position.

11. I have also served as a consultant to many technology companies over the course of my career. For example, starting in the early 2000s and continuously through the late 2010s I was a consultant to DivX, which was developing leading digital video solutions. As part of that work I worked closely with DivX engineers

on methods for encoding, packaging, delivering, and decoding video, including digital rights management (DRM).

B. Engagement

12. I have been retained by Patent Owner Ericsson AB (“Ericsson” or “Patent Owner”) to provide my opinions with respect to Ericsson’s Response to the Petition in *Inter Partes* Review proceeding IPR2025-00003, with respect to U.S. Pat. 9,313,178 (the ’178 patent). I am being compensated for my time spent on this matter at my standard rate. I have no interest in the outcome of this proceeding and the payment of my fees is in no way contingent on my providing any particular opinions.

13. As part of this engagement, I have also been asked to provide my technical review, analysis, insights, and opinions regarding the materials cited and relied upon by the Petition, including the prior art references and the supporting Declaration of Mr. Wechselberger.

14. The statements made herein are based on my own knowledge and opinions.

C. Materials considered

15. In preparing my opinions, I have reviewed and am familiar with the ’178 patent, including its written description, figures, and claims. I have also reviewed and am familiar with the Petition in this proceeding, the supporting

Declaration of Mr. Wechselberger, and the relied upon prior art and exhibits, including Peterka (Ex. 1005), Bochorov (Ex. 1007), Suzuki (Ex. 1006), and Peterka308 (Ex. 1008). I have also reviewed the materials cited in this declaration. My opinions are based on my review of these materials as well as my three decades of experience, research, and education in the field of art.

II. Relevant legal standards

16. I am not an attorney. I offer no opinions on the law. But counsel has informed me of the following legal standards relevant to my analysis here. I have applied these standards in arriving at my conclusions.

A. Person of ordinary skill in the art

17. I understand that an analysis of the claims of a patent in view of prior art has to be provided from the perspective of a person having ordinary skill in the art at the time of invention of the '178 Patent. I understand that I should consider factors such as the educational level and years of experience of those working in the pertinent art; the types of problems encountered in the art; the teachings of the prior art; patents and publications of other persons or companies; and the sophistication of the technology. I understand that the person of ordinary skill in the art is not a specific real individual, but rather a hypothetical individual having the qualities reflected by the factors discussed above.

18. I understand that the Petition applies a priority date of June 23, 2011 for the challenged claims, Pet. 7, and I apply the same date.

19. I further understand that the Petition defines the person of ordinary skill in the art at the time of the invention as having had a bachelor's in computer science, computer engineering, electrical engineering, or a related field, and 2-3 years of practical engineering experience relating to information security systems that employ cryptographic keys to encrypt/decrypt digital data. Pet. 9. The Petition adds that additional education could substitute for professional experience, or vice versa. *Id.* I do not dispute the Petition's definitions of a person of ordinary skill at this time, and my opinions are rendered on the basis of the same definition of the ordinary artisan set forth in the Petition, but I note that obviousness must be viewed from the perspective of one of ordinary skill in the field of information security using cryptographic keys for encryption and decryption of digital data, and my opinions are rendered on the basis of the definition of the ordinary artisan set forth in the Petition in view of that further clarification. I am at least a person of ordinary skill in the art under the Petition's definition.

20. Throughout my declaration, even if I discuss my analysis in the present tense, I am always making my determinations based on what a person of ordinary skill in the art ("the ordinary artisan") would have known at the time of the invention.

Based on my background and qualifications, I have experience and knowledge exceeding the level of the ordinary artisan, and am qualified to offer the testimony set forth in this declaration.

B. Burden of proof

21. I understand that in an *inter partes* review the petitioner has the burden of proving a proposition of unpatentability by a preponderance of the evidence.

C. Claim construction

22. I understand that in an *inter partes* review, claims are interpreted based on the same standard applied by Article III courts, *i.e.*, based on their ordinary and customary meaning as understood in view of the claim language, the patent's description, and the prosecution history viewed from the perspective of the ordinary artisan. I further understand that where a patent defines claim language, the definition in the patent controls, regardless of whether those working in the art may have understood the claim language differently based on ordinary meaning.

D. Obviousness

23. I understand that a patent may not be valid even though the invention is not identically disclosed or described in the prior art if the differences between the subject matter sought to be patented and the prior art are such that the subject matter

as a whole would have been obvious to a person having ordinary skill in the art in the relevant subject matter at the time the invention was made.

24. I understand that, to demonstrate obviousness, it is not sufficient for a petition to merely show that all of the elements of the claims at issue are found in separate prior art references or even scattered across different embodiments and teachings of a single reference. The petition must thus go further, to explain how a person of ordinary skill would combine specific prior art references or teachings, which combinations of elements in specific references would yield a predictable result, and how any specific combination would operate or read on the claims. Similarly, it is not sufficient to allege that the prior art could be combined, but rather, the petition must show why and how a person of ordinary skill would have combined them.

25. I understand that where an alleged motivation to combine relies on a particular factual premise, the petitioner bears the burden of providing specific support for that premise. I understand that obviousness cannot be shown by conclusory statements, and that the petition must provide articulated reasoning with some rational underpinning to support its conclusion of obviousness. I also understand that skill in the art and “common sense” rarely operate to supply missing

knowledge to show obviousness, nor does skill in the art or “common sense” act as a bridge over gaps in substantive presentation of an obviousness case.

III. The '178 Patent

26. United States Patent 9,313,178 (“the '178 Patent”), titled “Method and System for Secure Over-The-Top Live Video Delivery,” is directed to, among other things, “over-the-top (OTT) media delivery and more specifically key rotation for live streaming media.” Ex. 1001, 1:15-17.

27. The '178 Patent teaches that “[a]s content delivery models move away from streaming distribution over private networks to Web-based delivery of files over the public Internet, referred to as over-the-top (OTT) delivery, traditional content protection paradigms must be modified to support new delivery protocols, e.g., HTTP Live Streaming. For live streaming content with long or indefinite durations, use of a single encryption key for the entire duration increases the probability that the key may be compromised.” Ex. 1001, 1:18-26. “The generation of new strongly random values for use as content encryption keys and the rotation of content encryption keys provides protection from content encryption keys being compromised in long lived streams.” *Id.* at 3:2-5.

28. “A history of individual content encryption keys and the order in which they were generated is maintained.” *Id.* at 3:28-29. “Each content encryption key in

the history is assigned a unique identifier which is referred to herein as the content encryption key identifier.” *Id.* at 3:29-32.

29. “In one embodiment, when initiating playback of the stream, the client requests the current content encryption key, the next future content encryption key, and the fixed duration lifespan of the keys. The client uses the content encryption keys to decrypt the associated content.” *Id.* at 3:47-52.

30. “The transitioning between use of different keys is [] referred to herein as key ‘rotation.’” *Id.* at 1:63:65. “In step 310, the client 110 checks the expiration of current content key to see if a new key should be applied. There are two cases—normal period-based expiration, and an explicit key change notification received in step 308 that applies to the current segment being decrypted.” *Id.* at 11:3-7.

31. Claim 1 of the ’178 Patent is as follows. For consistency I will use the same claim element designations that were used in the Petition.

1PRE. A method for handling secure distribution of content comprising:
[1A] initiating a media playback request and receiving a playback request response;
[1B] parsing content information from the playback request response, the content information including content encryption keys, content encryption key identifiers, and content encryption key expiration times;

[1C] retrieving content and manifest files from a content delivery server;

[1D] detecting content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content;

[1E] issuing requests to a license server ahead of a key rotation boundary to retrieve a second content encryption key to be used after a content encryption key rotation boundary is reached; and

[1F] applying the second key for content decryption after the key rotation boundary is reached.

32. Claim 16 of the '178 Patent is as follows. For consistency I will use the same claim element designations that were used in the Petition.

16PRE. A computerized device operable as a client for handling secure distribution of content, comprising:

[16A] 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,

[16B] wherein the processors are operative to execute the computer program instructions from the memory to cause the computerized device to: initiate a media playback request and receive a playback request response;

[16C] parse content information from the playback request response, the content information including content encryption keys, content encryption key identifiers, and content encryption key expiration times;

[16D] retrieve content and manifest files from a content delivery server;

[16E] detect content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content;

[16F] issue requests to a license server ahead of a key rotation boundary to retrieve a second content encryption key to be used after a content encryption key rotation boundary is reached; and

[16G] apply the second key for content decryption after the key rotation boundary is reached.

IV. The Petition does not meet “parsing content information from the playback request response, the content information including content encryption keys. . .” as recited in all claims

A. Relevant claim language

23. Claim 1 of the '178 Patent recites “initiating a media playback request and receiving a playback request response.” *See* Limitation [1A] Claim 16 recites the same requirements. *See* Limitation [16B].

24. Claim 1 limitation [1B] further recites “parsing content information from the playback request response, the content information including content encryption keys.” Claim 16 limitation [16C] recites the same.

25. Under limitations [1B] and [16C], “the playback request response” must comprise ***multiple*** “content encryption keys.” The Petition acknowledges the same understanding. Pet. 23-25; Ex. 1003 ¶¶83, 86. In other words, as the Petition states, the challenged claims require that ***one “request”*** yields ***one “response”*** comprising ***multiple “content encryption keys”*** in the one response. Pet. 23-25; Ex. 1003 ¶¶83, 86.

26. Claim 1 limitations [1D] and [1F] further specify that the “content encryption keys” must be used/applied for decrypting content. *See* Pet. 23-24. Claim 16 limitations [16E] and [16G] recite the same.

B. The Petition's theory

27. According to the Petition, Peterka's "client-initiated requests to access media, e.g., program content," are each the "initiating a media playback request" of limitations [1A] and [16B]. Pet. 19-20; Ex. 1003 ¶¶ 76-77. The Petition further alleges that in Peterka, a *single* request for live media playback triggers a "response" in the form of *multiple* ECM and/or EMM messages, with each message containing what Peterka calls a "content key." Pet. 21-22. As I will explain further below, I do not agree with the Petition's characterization of Peterka.

28. The Petition maps Peterka's "content key" to the recited "content encryption key" of the challenged claims because Peterka's "content key" is used to decrypt the content, as the challenged claims require. Pet. 23-24. The Petition asserts that multiple ECM/EMM messages together (with one "content key" per message) allegedly meet the recited multiple "content encryption keys" of the challenged claims. Pet. 21-22.

29. The Petition relies exclusively on Peterka's "pull" embodiment, in which a client actively makes a request for each necessary key. Pet. 12, 18. On those bases, the Petition states that Peterka teaches providing *multiple* "content keys" in

response to a *single* “request” for live media, as claimed by the ’178 Patent. Pet. 21-22.

C. Peterka’s teachings contradict and refute the Petition’s theory

30. For the reasons detailed below, I disagree with the Petition’s theory. As I explain in detail below, I believe that the Petition and Mr. Wechselberger have mischaracterized Peterka’s teachings. Contrary to their assertions, Peterka’s “pull” embodiment does *not* teach providing *multiple* “content keys” in response to *one* client-initiated request for program content. Rather, as I show below, in all instances Peterka’s “pull” model provides *one* content key in response to each request for program content. Accordingly, the Petition’s theory cannot meet limitations [1B] and [16C], and thus fails as to all challenged claims.

31. Peterka discloses a multicasting system for distributing multimedia program content to client devices. Ex. 1005 ¶¶ 2, 6. Peterka teaches that multicasting “is similar to the existing TV broadcast” and “delivers the same content to one or more consumers at the same time,” such as “live content.” Ex. 1005 ¶ 58.

32. Peterka discloses three “purchase models” through which its system can provide content to clients: Pay-Per-View, Subscription, and Pay-By-Time. Ex. 1005 ¶¶ 63-82. As I explain below, all of the requests, responses, and different keys taught in Peterka are directed toward implementing its three “purchase models.”

Understanding Peterka's disclosure with respect to each purchase model is significant to understanding the Petition's errors.

33. Under Peterka's "**Pay-Per-View**" model, the client "purchases a single event" in its entirety. Ex. 1005 ¶63. To access and decrypt the pay-per-view content, the client "pulls" *one* "program key," and *one* "content key," *i.e.*, "*the* content key for that pay per view program." Ex. 1005 ¶105 (emphasis added). Peterka defines a "program key" or "PK" as the key-type "used to give access to an individual program event purchased using the pay-per-view option." *Id.* ¶98. Peterka defines a "content key" as the key-type "used to encrypt the content itself," *id.* ¶101, and to decrypt the content. *Id.* ¶¶106, 116, 121, 127; Pet. 11, 23-24. Under the Petition's theory, *only* the "content key"—and not the "program key"—constitutes a "content encryption key" for purposes of the challenged claims. Pet. 23-24. I note that Mr. Wechselberger acknowledged this fact at his deposition. Ex. 2011 at 37:14-20.

14	Q. Only Peterka's content keys are the
15	content encryption keys of your theory, right?
16	ATTORNEY SARWAR: Objection.
17	Form.
18	THE WITNESS: That's correct.
19	That was sufficient to support my opinions
20	of invalidity.

34. Peterka expressly teaches that each “pull” request for pay-per-view content results in a response containing only *one* content key. *Id.* ¶105. Peterka states: “Content keys, i.e., the keys used to encrypt the program content itself, are *not required to change* during a pay per view event. A client can pull a program key which is used to encrypt *the* content key for *that* pay per view program. Thus, *no other keys are required* during the pay per view event[.]” *Id.* (emphasis added). As Peterka states, that single content key comes along with a “program key” (PK) because a “program key” is the key-type used in Peterka to encrypt the content key for a pay per view event. *Id.* ¶¶ 98, 101, 105. Peterka describes this approach as “a multi-tier key hierarchy to accommodate the various purchase options such as pay per view or pay by time.” *Id.* ¶94. Thus, although Peterka teaches providing *two* keys in response to a pay-per-view request—a program key and a content key—only *one* of those keys is relevant to the Petition’s theory. Pet. 23-24; Ex. 2011 at 37:14-20. I note that Peterka never teaches providing more than one content key under the same program key, much less doing so in response to a single request.

35. Because Peterka’s Pay-Per-View model provides only *one* content key in response to *one* client-initiated “pull” request for content, Peterka’s pay-per-view

distribution model cannot meet limitations [1B] and [16C] and thus any challenged claim.

36. Peterka’s “**Subscription**” distribution model likewise teaches that a single content key is provided in response to a single client request. Under that model, the client “subscribes to the service,” and receives access to a variety of content. *Id.* ¶68. “[I]n the initial request under the subscription model, the client **requests** the subscription and pulls **a** service key encrypted under the unique key for that client.” *Id.* ¶105 (emphasis added). Thus, the client receives **one** “service key.” *Id.* The “service key” is Peterka’s key-type for the subscription distribution model. *Id.* ¶96. In response to its initial request under the subscription model, the client also receives a single “content key” that is “encrypted under a SK [service key] for those who are subscribers to the service.” *Id.* ¶101. Because the content key comes encrypted under the service key, and because the client’s initial subscription request yields only **one** service key, the client’s initial subscription request also only yields **one** content key. I note that Peterka never teaches providing more than one content key under the same service key, much less in response to a single request.

37. Indeed, Peterka expressly teaches that a client that has received its initial service key “may come back to the service and watch the content **without** negotiating **any** new keys” until its first service key has expired. Ex. 1005 ¶68

(emphasis added); *id.* ¶96 (“Once the client has ***the*** key, the client can decrypt the content of this service ***until the SK expires.***”) (emphasis added). The fact that the client does not need to negotiate “***any*** new keys” during the lifespan of its first service key further shows that the client receives only ***one*** content key in response to an initial subscription model request.

38. Peterka further teaches that the service key has “a duration from several days to several months.” *Id.* ¶96. Thus, Peterka teaches that in the Subscription model, the client’s “request” receives a response with ***one*** service key and ***one*** content key that the client may use for several days to several months.

39. Moreover, Peterka further teaches that to receive a next service key upon expiration of the initial service key, “the client ***requests*** the next version of the SK from the caching server.” *Id.* ¶96 (emphasis added). The next single content key would again be sent encrypted under the new service key. *Id.* ¶ 101.

40. Thus, under the Subscription model (like the Pay-Per-View model), each “pull” “request” produces a response providing ***one*** relevant key (one content key encrypted under one service key), and not multiple “content encryption keys” as required by the ’178 Patent’s challenged claims. Accordingly, Peterka’s

Subscription distribution model also cannot meet limitations [1B] and [16C], and thus the challenged claims.

41. Peterka's **Pay-By-Time** model likewise only provides a single content key in response to a single client-initiated "pull" request. Under the Pay-By-Time model, a client purchases one or more time segments of content, and "pays for the duration of the content that was actually watched." Ex. 1005 ¶53. "At the time the viewer negotiates the purchase options with the OCS [origin content server], the viewer may choose to select the pay-by-time option if offered. The viewer will be told what the pay periods are and what the cost of each pay period is. The viewer's selection will be included in a secure object." *Id.* ¶ 81 (bracketing added).

42. Under the Pay-By-Time model, the first segment of content that the client may access is a "**free preview.**" *See, e.g.,* Ex. 1005 Figs. 7A, 7B.

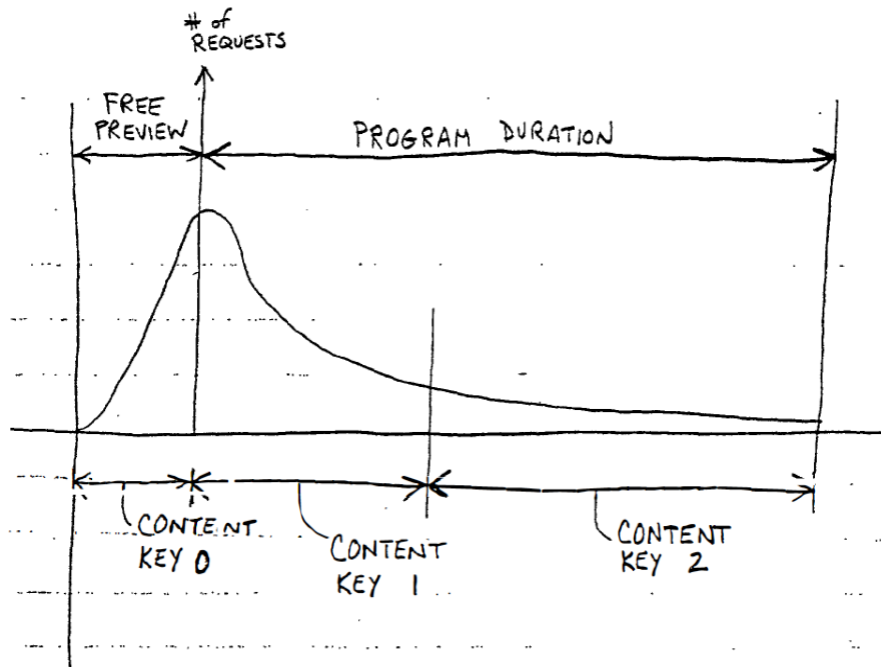


Fig. 7A

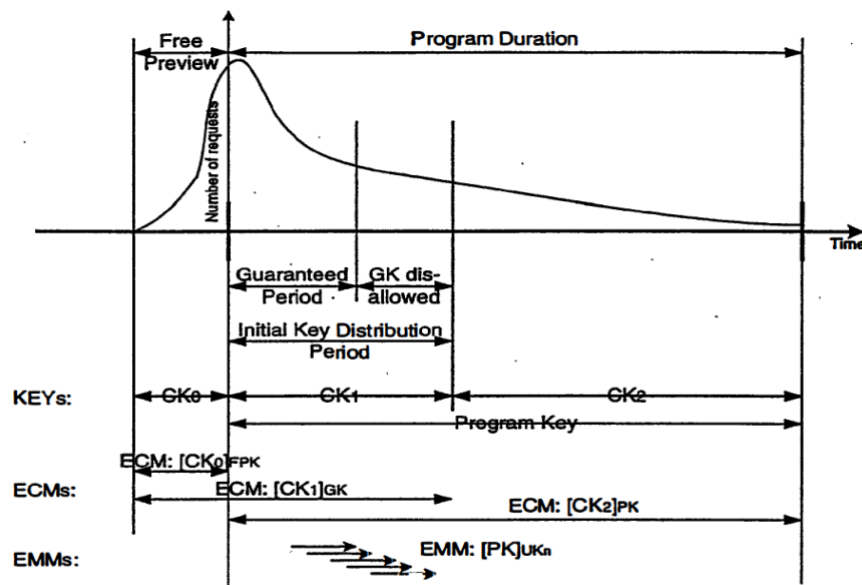


Fig. 7B

43. The “free preview” is, for instance, “a movie trailer prior to broadcast of the actual movie or an advertisement for the program material or a first portion of the actual movie.” *Id.* ¶ 9.

44. To decrypt the free preview segment, the client may need a content key. *Id.* ¶85. However, Peterka teaches that the client receives any necessary content key *without* making any “request” for that content key because the content key “is provided *ahead of time*, for example, during provisioning.” *Id.* ¶83. This is because clients do not initiate a request for “free preview” content; rather, the free preview content is provided to clients as an advertisement or enticement for them to purchase paid content. To that end, Peterka repeatedly underscores that the content key for the free preview period is provided to clients *without request*. *Id.* ¶84 (“a free preview key is provided *ahead of time*, e.g., during provisioning, to a client as shown in block 420.”) (emphasis added); *id.* ¶85 (“In block 408, a content key is provided. The content key is encrypted with a free preview key as shown in block 412. The encrypted content key is then provided to the plurality of clients as shown by block 416.”); *id.* ¶103 (defining “Free Preview Key (FPK)” as a key “used to distribute the CK [content key] or the PSK [program segment key] that in turn encrypts the CK for the content during the initial free preview period. This may be a *fixed key known to all clients or distributed during provisioning*.”) (emphasis and bracketing added).

45. The *unrequested* content key provided for the “free preview” segment allows the client “to decrypt the program material and obtain a preview of the program without charge.” *Id.* ¶ 83.

46. In the illustrations and descriptions of Figs. 7A and 7B, this first *unrequested* content key for the “free preview” segment is labeled as CK0, “content key 0,” or “Key 0.” Ex. 1005 Figs. 7A & 7B, ¶¶ 92, 93, 122.

47. Because Peterka provides the content key for the free preview segment without request, this key (e.g., CK0 in Figs. 7A & 7B) cannot meet limitations [1B] and [16C] and thus cannot meet the challenged claims.

48. Under Peterka’s Pay-By-Time model, the next segment of content available to a client is an “**Initial Viewing Period.**” Ex. 1005 ¶90 (describing the “initial viewing period” as immediately following the “free preview period”); *id.* ¶93 (with respect to Fig. 7A, describing the segment after the “free preview period” as the “initial viewing period”). Peterka states that the “initial viewing period” is equivalent to the “initial key distribution period” shown in Figure 7B. *Id.* ¶131 (with respect to Figure 7B, stating that the period defined by CK1 “is called the initial viewing period, or *equivalently*, the initial key distribution period.”) (emphasis added).

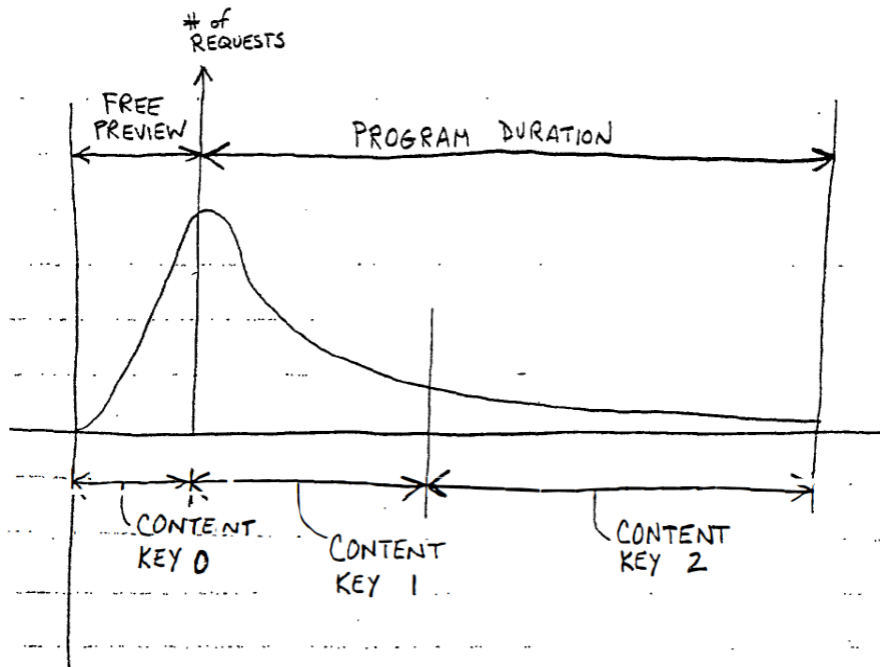


Fig. 7A

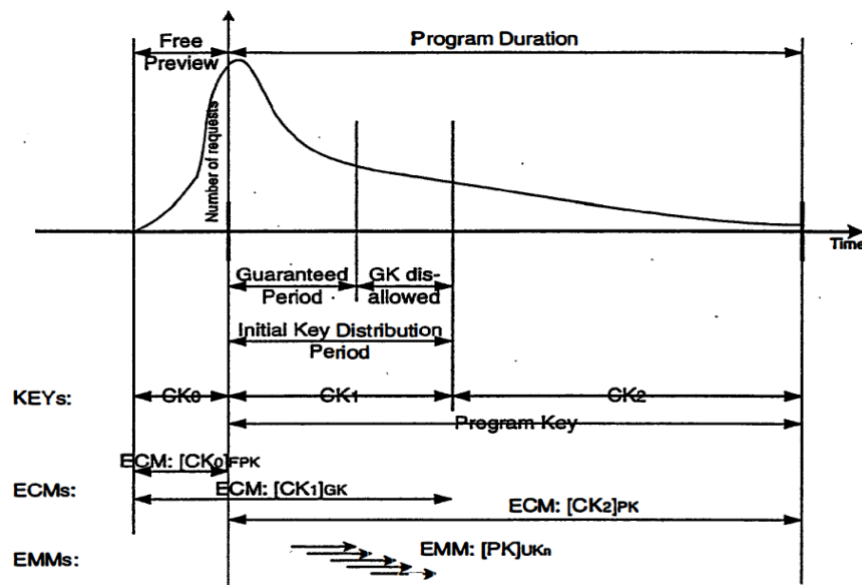


Fig. 7B

49. To access the “initial viewing period,” clients are provided a “group key” and a “content key” encrypted under the group key. *Id.* ¶127 (describing the key distributed to clients for accessing the “initial viewing period” as “referred to herein as a group key,” and further teaching that a “second key,” “referred to as a content key,” is encrypted under the group key and provided to clients for decrypting the “initial viewing period” content); *id.* ¶102 (defining “Group Key” or “GK” as the “key used to distribute the CK [content key] or the PSK [program segment key] that in turn encrypts the CK for the initial viewing period.”) (bracketing added); *id.* ¶93 (with respect to Fig. 7A, stating: “Key 1 would represent a group key itself or a content encryption key encrypted under the group key used during the initial viewing period.”); *id.* ¶122 (“Fig. 7B shows an entitlement control message in which a content key is encoded with a group key (ECM:[CK1]GK).”).

50. Importantly, Peterka repeatedly and consistently teaches that clients are also given the content key for the “initial viewing period” *without request* because this content key is also provided to clients ahead of time, encrypted under the Group Key. Ex. 1005 ¶102 (“Clients will get the GK [group key] ahead of program events sold on PPV [pay-per-view] or PBT [pay-by-time] basis, for instance during the provisioning.”); *id.* ¶127 (“One method of implementing an initial viewing period is to distribute a common key to potential participants ahead of time, e.g., *prior to*

distribution of program content. Such a key is referred to herein as a group key.”) (emphasis added); *id.* (“Since *every client* would receive a group key in such a situation, all clients could, in theory, receive the first part of the content for free.”)¹ (emphasis added); *id.* ¶128 (“the group key is distributed *ahead of time*”); *id.* ¶59 (stating that the “group key” is “*known in advance* to registered clients”) (emphasis added); *id.* ¶127 (further teaching that the “content key” for decrypting the “initial viewing period” is also provided to clients with the group key, prior to any request for the content from the clients); *id.* ¶102 (defining “Group Key” or “GK” as the “key used to distribute the CK [content key] or the PSK [program segment key] that in turn encrypts the CK for *the initial viewing period.*”) (emphasis added); *id.* ¶93 (with respect to Fig. 7A, stating: “Key 1 would represent a group key itself or a content encryption key encrypted under the group key used during the initial viewing period.”); *id.* ¶122 (“Fig. 7B shows an entitlement control message in which a content key is encoded with a group key (ECM:[CK1]GK).”).

51. Thus, in Peterka’s Figs. 7A and 7B, Content Key 1 (CK1)—the content key for the initial viewing period or initial key distribution period—is provided to

¹ Peterka’s reference to “first part of the content” here refers to the initial viewing period, as the surrounding teachings in Paragraph 127 make clear; it does not refer to the earlier “free preview period,” which is not necessarily “the content,” but may instead be a trailer or advertisement for the content. Ex. 1005 ¶ 9.

Peterka's clients without request. That remains true regardless of whether the client eventually uses a "pull" model to request a content key, because at this stage there has been no client-initiated content key request, and thus there has been no "pull."

52. Peterka explains its reasons for providing the initial viewing period content key (CK1 in Fig. 7B) without request in its rationale for its "initial viewing period." Ex. 1005 ¶90. As Peterka explains and illustrates through Figures 7A and 7B, most clients are expected to request (i.e., purchase) Pay-By-Time content toward the end of the free preview period and in the beginning of the "initial viewing period" (equivalent to the "initial key distribution period" in Fig. 7B). *Id.* ¶91; Figs. 7A, 7B. Peterka teaches that if clients have not already been provided the content key for the first content segment after the free preview (i.e., CK1 in Figs. 7A and 7B), many clients who choose to purchase that content segment will face a service interruption because there would not be "enough time to communicate with the server, and receive the key necessary to decrypt" that segment. *Id.* ¶90. To avoid that problem, Peterka teaches that "[t]he initial viewing period concept invention provides a way to enable continuous viewing despite the latency in server key distribution." *Id.* As Peterka explains, providing the content key to the "initial viewing period" to clients ***without request*** "allow[s] viewers to receive the beginning of a program during this period when the server is distributing keys to those who have purchased the program

material.” *Id.* ¶126. Peterka acknowledges that by giving every client the content key for the initial viewing period *without request*, all clients can view that content segment for free. *Id.* ¶127 (“Since every client would receive a group key in such a situation, all clients could, in theory, receive the first part of the content for free.”); *id.* ¶133 (“a first portion of the program content is multicast to a plurality of clients at no charge”). However, Peterka teaches that this can be mitigated by appropriately defining the length of the “initial viewing period” based on client demand for the paid portion(s) of the content. *Id.* ¶ 133.

53. Because Peterka provides the content key for the “initial viewing period” segment *without request*, this key (e.g., CK1 in Figs. 7A & 7B) also cannot meet limitations [1B] and [16C] and thus cannot meet the challenged claims.

54. Rather, Peterka teaches that the first *requested* content key that a client receives for Pay-By-Time content is the content key for the segment *after* the “initial viewing period.” *Id.* ¶93. For purposes of Figures 7A and 7B, this first requested content key is labeled **Content Key 2** (CK2). Ex. 1005 ¶93 (“Key 2 would be the *actual* content encryption key delivered *only* to those clients that *purchased* the content. Thus clients that tune to the content first view a free preview, and make a decision to buy. Those who make such requests use the group key [already provided] to allow their viewing experience to continue. The server would deliver Key 2 during

this time, so that those viewers could continue viewing the remainder of the content in a continuous fashion.”) (emphasis and bracketed text added). As Peterka thus teaches, the client’s first “*request*” for content in a Pay-By-Time model corresponds to its decision to purchase a content segment, and the first content key provided in *response* to such a purchase request is **Content Key 2** (CK2). *Id.* ¶¶ 93, 129-131.

55. Moreover, Peterka’s teaching discloses that the Pay-By-Time distribution model operating in “pull” mode only provides *one* content key in response to each client request.² Peterka teaches that in “pull” mode, “a server receives a request for *a* cryptographic key,” and “logs the request for *the* key,” *i.e.*, *one* key. Ex. 1005 ¶106 (emphasis added). “[T]he key and its expiration time are distributed to the client in response to the request by the client.” *Id.* Under the pull model, “the responsibility of determining when *a* new key is required can be passed to the client,” and “program content is distributed for decryption by the client utilizing *the* cryptographic key that was requested.” *Id.* (emphases added). Peterka later reiterates: “Under a pull key distribution model, each client requests *a* new key and is individually responded to by the key distribution server.” *Id.* ¶110 (emphasis

² As noted, the Petition expressly states that all of its Grounds rely *exclusively* on Peterka’s *pull model*. Pet. 11-12 (“The Grounds herein rely on Peterka’s *pull model*.”) (emphasis Petition’s); Pet. 18 (“Every element of claims 1 and 16 is satisfied by or obvious over Peterka’s pull method.”).

added). Peterka additionally teaches that a client “can monitor the expiration time of the program segment key and send an *individual* key update request before *the* key expires. Again, this is a way of implementing the ‘pull’” model under Peterka’s teachings. *Id.* ¶114. Thus, under Peterka’s “pull” mode, each client request receives *one* key in response to each request, and a client must make a new request each time it seeks a new key. Peterka’s Figure 8, which depicts the operation of its “pull” mode, further underscores that Peterka operates in this manner.

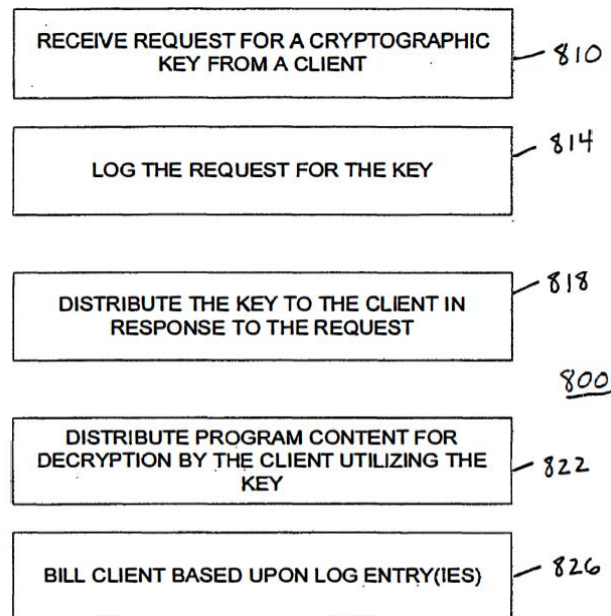


Fig. 8

56. A client that purchases content through Peterka’s Pay-By-Time distribution scheme using Peterka’s “pull” mode will thus request a *single* new

content key for each next paid content segment it wishes to purchase, and will receive that *single* content key in response.

57. The Petition alleges that “Peterka teaches distributing *multiple* keys (e.g., multiple ECMs) to a client—e.g., for the current *and* next media segment—in response to such a request.” Pet. 12 (emphasis original) (citing Ex. 1005 ¶¶ 80, 130, Fig. 7B, Ex. 1003 ¶¶ 50-51); Pet. 20 (additionally citing Ex. 1005 ¶ 53, Ex. 1003 ¶ 77); Pet. 22, 25-26. I disagree. The Petition’s assertion and Mr. Wechselberger’s corresponding opinions rely on a misinterpretation of Peterka.

58. While Peterka does indeed teach distributing multiple keys in multiple ECMs to a client, including for a current and next segment, Peterka does *not* teach distributing multiple *content* keys (the only relevant key type) in response to a *single* “pull” request, as the Petition alleges and its theory requires. Ex. 2011 at 37:14-20.

59. For instance, in Fig. 7B, Peterka shows a first ECM carrying Content Key 0 (CK0) encrypted under a free preview key (FPK), and a second ECM carrying Content Key 1 (CK1) encrypted under a group key (GK). Those two content keys are for a current segment (free preview) and next segment (initial viewing period or initial key distribution period). However, as I explained in detail above, *neither* was provided in response to any “*request*.” See ¶¶ 41-52, *supra*. Rather, both content keys were provided “ahead of time,” before any client-initiated request for content.

See ¶¶ 44, 50, *supra*. The first ***requested*** content key in Figure 7B is Content Key 2 (CK2). See ¶54, *supra*. But Peterka expressly teaches that Content Key 2 is the ***last*** content key that will be provided in the embodiments of Figures 7A and 7B. Ex. 1005 ¶92 (“Content keys 1 and 2 illustrate an example where only two keys are required to decrypt the remainder of the program content.”). Content Key 2 is thus the ***only requested*** content key that is provided for purposes of Figures 7A and 7B. Accordingly, the Petition cannot meet the challenged claims—which require ***multiple*** content encryption keys in a single request response (limitations [1B] and [16C])—based on the embodiments of Figures 7A and 7B.

60. The Petition’s reliance on the statement in Peterka that “each rabbit³ is given keys to the current as well as the next segment,” Ex. 1005 ¶80, likewise does not support the Petition’s assertions. In that passage, Peterka does not teach providing content keys to two segments ***in response to a single request***, as the challenged claims require and the Petition contends. Paragraph 80 of Peterka is addressing an entirely separate issue—the ***timing*** of each request for a new content key and the timing of each response providing a new content key—and explaining that the key for the next segment will be provided during the current segment in order to avoid service interruptions. *Id.* This is consistent with Peterka’s teachings

³ This is a typo in Peterka and presumably was intended as “client.”

as to Figure 7B, where the content key for the initial viewing period (Content Key 1) is provided during the free preview period to avoid service interruptions. Peterka's paragraph 80 thus does not support the Petition's assertion that Peterka teaches providing multiple *content keys* in response to *one* "pull" request. For the same reasons, I disagree with Mr. Wechselberger's interpretation of Peterka's paragraph 80. Ex. 1003 ¶¶ 52, 77, 100.

61. For the same reasons, I believe the Petition also misinterprets paragraph 130 of Peterka. That is directed to its teaching of a "guaranteed period," as illustrated in Figure 7B.

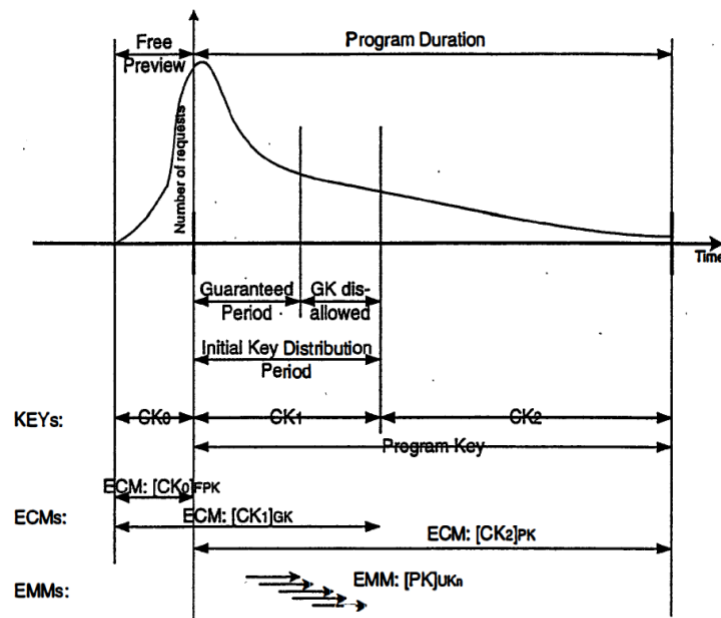


Fig. 7B

62. The “guaranteed period” is a sub-set of the initial viewing period (or “initial key distribution period”) as Figure 7B illustrates. *Id.* ¶130 (“the initial key distribution period is shown lasting longer than the guaranteed period”). The “guaranteed period” does not support the Petition’s assertion that a *single request* receives *multiple* content keys in Peterka. Rather, Peterka explains that the “guaranteed period” defines the time in which clients can request *a single* content key for the *next* segment (Content Key 2 or CK2) and receive that *single* key *during* the current segment (the initial viewing period) to avoid service interruptions. *Id.* ¶130. The “guarantee” thus conveys the assurance that if the client makes its request within the guarantee period, the client’s viewing experience will be uninterrupted. *Id.* ¶130 (“Thus, the *next* content key will have been obtained by a purchasing user *prior* to the initial key distribution period *elapsing*.”) (emphasis added); *id.* ¶131 (“Thus, to provide a satisfying user experience, all clients who request access to an event . . . during the ‘guaranteed period’ will be guaranteed to receive the content without interruption.”). Thus, paragraph 130 of Peterka simply provides a more detailed explanation of its teaching as to providing a content key for a next segment during a current segment to avoid service interruptions. But as shown with respect to the embodiment of Fig. 7B and Peterka’s “pull” mode more broadly, each “request” only yields *one* content key in response. *See* ¶¶ 41-54, *supra*. Peterka’s

paragraph 130 thus does not support the Petition’s assertion that Peterka teaches providing multiple *content keys* in response to *one* “pull” request. For the same reasons, I believe Mr. Wechselberger has misinterpreted paragraph 130 of Peterka. Ex. 1003 ¶¶ 52, 77, 100.

63. For the reasons above, the Petition and Mr. Wechselberger also misinterpret Peterka’s Figure 7B, alleging that it “shows two content keys CK0 and CK1 distributed in separate ECMs for *each request* received during a free preview period [], and two content keys CK1 and CK2 distributed in separate ECMs for *each request* received during an initial key distribution period [].” Pet. 20-22 (emphasis added); Ex. 1003 ¶78. As explained above, CK0 and CK1 are both distributed *without request*. See ¶¶ 41-53, *supra*. CK2 is the only single content key distributed in response to a request, and this cannot meet the challenged claims (limitations [1B] and [16C]). See ¶ 54, *supra*.

64. I also note that the Petition cites to Peterka’s paragraph 53, Pet. 20, but this paragraph provides a very general description of Peterka’s pay-by-time distribution model, and teaches nothing about providing multiple content keys in response to one request, as the Petition contends.

65. In addition, I believe that the Petition and Mr. Wechselberger misinterpret the Peterka statement that, under its “pull” model, “each client keeps

track of the keys and their expiration times and actively requests new keys before the current keys expire so as to avoid service interruptions.” Ex. 1005 ¶105 (emphasis added). Mr. Wechselberger cites to this teaching in support of his opinion that Peterka teaches limitations [1B] and [16C]. Ex. 1003 ¶51. That statement from paragraph 105 of Peterka, however, does not disclose requesting or receiving multiple **content** keys, which is the only relevant key type for the Petition’s theory. Pet. 23-24. Rather, as explained above, Peterka teaches that **content** keys are encrypted under at least one **other** key corresponding to the relevant distribution model for the requested content. Ex. 1005 ¶101 (Teaching that the content key can be distributed “(1) encrypted under the PSK for those viewers who select the pay-by-time option, (2) encrypted under the PK or UK for users who select the PPV option; or (3) encrypted under a SK for those who are subscribers to the service.”). Peterka’s reference to requesting **multiple** “keys” in connection with its “pull” model, Ex. 1005 ¶105, is thus directed to requesting and obtaining **one** content key and at least **one** other non-content key under which the content key is encrypted, such as a “program key” for pay-per-view content. *Id.* ¶105 (“A client can pull a program key which is used to encrypt **the** content key for that pay per view program. Thus, **no other keys are required** during the pay per view event[.]”) (emphasis added). Peterka illustrates this approach in the embodiment of Figure 7B, which

shows that content key 2 (CK2) is provided in an ECM message encrypted under a program key (PK), which is the key for pay-per-view distribution. Although two keys are sent in the ECM message that transports CK2, there is only *one* content key. Accordingly, Peterka’s paragraph 105 does not teach that a client’s single “pull” request receives *multiple content keys* in response, as the Petition’s theory requires. Ex. 2011 at 37:14-20.

66. I understand that the Petition and Mr. Wechselberger have also alleged it would have been obvious to an ordinary artisan “to package multiple keys/entitlement messages (ECMs or EMMs) into a ‘single’ ‘combined’ ‘*multicast message*,’” Pet. 22, 28 (citing Ex. 1003 ¶¶ 81, 101).

67. I disagree. As a threshold matter, in Peterka’s pay-per-view model, a client can only request *one* content key (e.g., CK2 in Figs. 7A and 7B), which lasts for the remaining duration of the pay-per-view event. See ¶¶ 33-35, 50, *supra*. This is shown in Figure 7B, where a single content key (CK2) is sent encrypted under a single program key (PK)⁴ in response to the first and only client-initiated request for content. Fig. 7B; *Id.* ¶¶ 92-93. Thus, it would not have been obvious to package and

⁴ As explained, a program key is Peterka’s key-type for pay-per-view content. *Id.* ¶98.

send multiple content encryption keys in response to a client-initiated request for pay-per-view content.

68. Moreover, under Peterka’s Subscription model, the client receives one content key that lasts for several days to several months. *See* ¶¶ 36-38, 40, *supra*. Clients have ample time to request the next content key “adequately far enough in advance so as to avoid overloading the server.” Ex. 1005 ¶96. There is thus no need to send the client additional content keys for future subscription periods that are many days or months away.

69. To the contrary, as explained below, an ordinary artisan would find the Petition’s obviousness modification undesirable and non-obvious for both the Subscription model and the Pay-By-Time model in view of Peterka’s teachings and the design of Peterka’s system.

70. The Petition’s proposed modification requires sending clients a “single combined *multicast* message” containing multiple content encryption keys for successive segments or subscription periods. A “multicast message” is a single message that is sent to *multiple* clients simultaneously. *See* <https://en.wikipedia.org/wiki/Multicast#:~:text=In%20computer%20networking%2C%20multicast%20is,point%2Dto%2Dmultipoint%20communication> (accessed

July 1, 2025). As Peterka itself states, its “multicast messages” are “group-addressed.” Ex. 1005 ¶ 104.

71. Using a multicast message to send multiple content keys for successive content periods to a group of clients in Peterka’s system would create significant problems of over-inclusivity and under-inclusivity in content key distribution that would render Peterka’s modified system more inefficient than it was without modification, or at least certainly no more efficient.

72. The Petition’s proposed modification would create an *over*-inclusivity problem because sending “a single combined multicast message” with *multiple* content keys for multiple segments (pay-by-time model) or multiple subscription periods (subscription model) to multiple clients would give certain clients access to additional future content that they *did not purchase*, thus defeating the purpose of Peterka’s pay-by-time and subscription models. By way of example, suppose that ten clients have requested to purchase segment 2, but only eight of them have requested to purchase segment 3, and only four of them have requested to purchase segment 4. Under Peterka’s existing approach, three multicast messages would be sent: a first message to all ten clients, containing one content key to segment 2; a second message to only eight clients containing one content key to segment 3; and a third message to only four clients containing the content key to segment 4. Under

the Petition’s approach, however, one message would be sent to all ten clients, providing three content keys to each client for segments 2, 3, and 4. As a result, six of the ten clients would receive content keys to segments they did not purchase—defeating the purpose of Peterka’s pay-by-time model. While the number of messages sent has decreased from three to one, the ability to sell distinct content segments to distinct clients according to their distinct purchase requests has broken down, and an ordinary artisan would not find this desirable or even “efficient” in view of Peterka’s teaching and purpose.

73. The Petition’s proposed modification would also create an *under-inclusivity* problem because the multicast message for multiple future content keys would be sent *before* eventual new clients have joined the multicast distribution group. For instance, in the context of the Pay-By-Time model, Peterka provides use-case examples including “fashion shows” and “sustained sports events (e.g. Olympics).” *Id.* ¶78. These are events with long durations that do “not have a well defined start or end time or a self-contained plot[.]” *Id.* Accordingly, well after the start of the live stream event, new clients will decide to purchase discrete content segments (e.g., the portion of the fashion show for a particular brand of interest, or a particular event at the Olympics). Under the Petition’s modification, Peterka’s system will have *already* sent out the content key(s) for the segment(s) these new

clients seek in a multicast message that *did not include them* because it was sent before these clients made the content request. For instance, under the Petition's modification, clients who request to watch a segment of a fashion show mid-way through the show will not have received the content key for that segment that was sent to other clients earlier. As a result, a new message will have to be sent, defeating the Petition's alleged "efficiency" motivation for the modification. Similarly, in the context of the Subscription service, the Petition's modification would mean that the content key(s) for future subscription periods would have already been sent before certain new subscribers joined. To remedy this under-inclusivity problem, Peterka's system would again have to send out a new multicast key distribution message to these new clients. The Petition's proposed modification would thus not render Peterka's system more "efficient," as the Petition and Mr. Wechselberger have alleged. Pet. 22; Ex. 1003 ¶ 81.

74. The Petition further contends that Peterka itself teaches the Petition's proposed modification as a "viable option." Pet. 22 (citing Ex. 1005 ¶¶ 104, 121). As a threshold matter, I understand that the Petition must prove that the proposed modification would have been, on whole, *desirable* to the ordinary artisan at the time of the invention, including in view of the associated downsides and not simply based on the existence of some potential advantage. My understanding is that an allegation

that the modification was merely *viable* does not suffice to provide a motivation or show obviousness. Stated otherwise, viability speaks to what could have been done, not what an ordinary artisan would have been motivated to do.

75. Nonetheless, the cited passages in Peterka (paragraphs 104 and 121) also do *not* teach or suggest the proposed modification, i.e., they do not teach or suggest packaging multiple *content keys* for *successive* periods and providing them in a multicast message to multiple clients.

76. Peterka's paragraph 104 teaches that multiple different keys, each intended for "*individual clients*" and encrypted under each client's "Unique Key" or "UK," can be "combined into a single multicast message" and sent to multiple clients at once, leaving each intended client to identify and obtain the key directed to it. *Id.* ¶104. As Peterka later specifies, in this scenario "a user identification" must often be included in such a packaged EMM. *Id.* ¶120. This is to allow each client to identify the individual key directed to it. By way of analogy, the teaching in Peterka's paragraph 104 is akin to sending seven boxes each containing seven keys for seven different individuals to seven different addresses. Because each of the seven keys is only useful to *one* recipient, each recipient would open the box,

identify the one key with their name on it, and have no use for the other six. Thus, no recipient would truly receive anything they were not supposed to have.

77. By contrast, the Petition’s proposal requires placing multiple *content* keys for multiple *successive content periods* into one message and multicasting that message to multiple clients at once. The Petition’s proposed modification is thus akin to sending seven boxes each containing seven keys to seven individuals who can each use *all seven keys* but who may only have paid for the access associated with one or two of the keys. As explained earlier, this would create an over-inclusivity problem that would defeat Peterka’s distribution models. An ordinary artisan thus would not have found the Petition’s modification obvious or desirable in view of the intended purpose of Peterka’s teachings.

78. The Petition has also cited to Suzuki at paragraphs 76 to 77 as allegedly teaching that “multiple keys were conventionally transmitted in one message in response to a client request.” Pet. 22. I disagree with that assertion. Suzuki’s paragraphs 76 and 77 do not teach transmitting multiple “*content encryption keys*,” as recited in the challenged claims. Rather, those paragraphs disclose providing “key *information* relating to the key currently in use (key A) and the next key to be used (key B).” Ex. 1006 ¶¶ 76-77. Moreover, Suzuki is not directed to a pay-by-time, pay-per-view, or subscription distribution model, in which a content key grants access to

content that different clients must individually decide to purchase in discrete units or increments, as in Peterka. Thus, Suzuki could not motivate providing Peterka's clients with content keys to content they did not agree to purchase.

79. Accordingly, the Petition does not meet or render obvious limitations [1B] and [16C] under its theories with respect to any Grounds.

V. The Petition does not meet “parsing content information from the playback request response, the content information including . . . content encryption *key identifiers*” as recited in all claims

A. Relevant claim language

80. Claim 1 limitation [1B] and claim 16 limitation [16C] further recite “parsing content information from the playback request response, the content information including . . . content encryption *key identifiers*.”

81. The '178 Patent states: “A history of individual content encryption keys and the order in which they were generated is maintained. Each content encryption key in the history is assigned a unique identifier which is referred to herein as the content encryption key identifier.” Ex. 1001 at 3:28-32.

82. The ordinary artisan would have understood the above statement from the specification to define the claimed “content encryption key identifiers.” That definition is not directed to only one embodiment or some embodiments, but rather defines *all* “content key encryption identifiers” across any embodiment. The phrase

“referred to herein” further makes clear the definitional nature of the specification’s teaching in this context.

83. The specification imposes two requirements for “content encryption key identifiers”: (1) each content encryption key identifier must be “*unique*” in the context of *all* content encryption keys maintained in the “history,” and (2) each content encryption key identifier must be “*assigned*” to the corresponding content encryption key *itself*. This second requirement is further confirmed by the words “*key* identifier.”

B. The Petition’s theories

84. The Petition initially alleges that Peterka’s teaching of “a sequence number or a time stamp” assigned to ECM/EMM messages, Ex. 1005 ¶121, meets the recited “content encryption key identifier” of the challenged claims. Pet. 25. The Petition contends that Peterka’s ECM/EMM time stamps or sequence numbers are unique to each ECM/EMM message, and each ECM/EMM “carries a different content encryption key.” *Id.* On those bases, Mr. Wechselberger states that Peterka’s message sequence numbers or timestamps “*can be used* to uniquely identify the key that was in the ECM or EMM.” Ex. 1003 ¶ 91.

85. The Petition alternatively alleges it would have been obvious to modify Peterka to “use a key identifier to identify the content key in an ECM/EMM.” Pet. 26.

86. The Petition further alleges it would have been obvious to combine Peterka with Suzuki to add key identifiers to Peterka’s client request response. Pet. 51-53.

87. With respect to claims 7-8 and 19, the Petition’s Ground 5 further proposes a four-reference combination that would include the use of timestamps as content key encryption identifiers to allow clients “that held keys for multiple future segments” to determine “which key to apply at the next rotation boundary.” Pet. 69.

C. Peterka’s message sequence numbers or timestamps are not “content encryption *key* identifiers”

88. As explained above, the “content encryption key identifier” of the challenged claims must be “*assigned*” to the corresponding content encryption *key* itself. Ex. 1001 at 3:29-32.

89. Peterka’s sequence numbers or timestamps, however, are assigned to its ECM/EMM *messages*, and not the content key included in each such message. Ex. 1005 ¶121 (teaching that the disclosed sequence number or time stamp is provided under “a format for such messages”). The Petition itself recognizes this fact, and states: “the sequence number/timestamp is unique to *each* ECM/EMM[.]”

Pet. 25 (emphasis added). Thus, Peterka’s sequence numbers or time stamps are not the claimed “content encryption *key* identifiers”; they are instead *message* identifiers, which cannot meet the challenged claims.

90. Mr. Wechselberger’s testimony confirms this distinction. At his deposition, Mr. Wechselberger acknowledged that Peterka’s sequence numbers or time stamps are “*tied to the ECM or EMM[.]*” Ex. 2011 at 38:14-20 (emphasis added). Moreover, Mr. Wechselberger stated in his declaration that Peterka’s sequence numbers or time stamps “*can be used* to uniquely identify the key that was in the ECM or EMM,” Ex. 1003 ¶91 (emphasis added), further acknowledging that they are not assigned to the relevant *key* in Peterka’s message, but instead are merely *message* identifiers.

91. My opinion is further confirmed by the Petition’s proposed obviousness modification in Ground 1. The Petition states: “POSITAs would have been motivated . . . to implement Peterka’s client *to receive and use a key identifier* to identify the content key in an ECM/EMM.” Pet. 26 (emphasis added). This statement in the Petition acknowledges that Peterka’s sequence numbers or timestamps for its ECM/EMM messages are *not* key identifiers for the reasons explained above, i.e., they are not *assigned to content encryption keys*, as the challenged claims require.

92. Separately, I further note that in Peterka’s “pull” model, which is the only relevant key distribution scheme for purposes of the Petition, each content key request receives only one key in response, as I have explained above. *See* Section IV.C, *supra*. Accordingly, Peterka also does not teach a request response that includes **multiple** “content encryption key identifiers” as the challenged claims require.

D. The Petition fails to demonstrate obviousness with respect to “content encryption key identifiers”

93. I further disagree with each of the Petition’s obviousness allegations with respect to the recited “key identifiers,” and find that the Petition’s stated motivations for its obviousness modifications would not have (and could not have) motivated a person of ordinary skill in the art to make the proposed changes.

94. In Ground 1, the Petition argues that Peterka’s Figure 7B “**shows** delivery of content keys with unique designations—CK0, CK1, CK2,” and that this would have motivated the ordinary artisan to “use a key identifier to identify the content key in an ECM/EMM.” Pet. 26 (emphasis Petition’s). I disagree. Peterka uses CK0, CK1, and CK2 as descriptive labels for purposes of the teachings of its specification; it provides no teaching that any such labels are actually sent to the client as key identifiers. Moreover, the Petition itself alleged that Peterka can **already** identify content keys by **using** the allegedly unique sequence numbers or time

stamps assigned to each *message* carrying each different content key. Pet. 25. That statement thus contradicts the Petition’s purported motivation that “POSITAs would have recognized the need to differentiate between keys” in Peterka’s unmodified system. Pet. 26. Put another way, according to the Petition, and Mr. Wechselberger, Peterka’s system *already* allowed for differentiation between keys, albeit using *message* identifiers that do not meet the recited “*key* identifiers” of the challenged claims. Pet. 25, Ex. 1003 ¶91. Thus, the Petition has not identified any benefit or improvement to Peterka’s system from adding key identifiers that would have motivated an ordinary artisan to do so, and I disagree that the ordinary artisan would have found such a modification obvious.

95. For similar reasons, I disagree with the Petition’s obviousness theory in Ground 2, based on the combination of Peterka and Suzuki. The Petition contends that “[a] POSITA would have recognized the importance of [key] identifiers to differentiate amongst keys, and that providing unique values (*such as* key numbers) to keys would ensure that the system does not confuse keys.” Pet. 52-53 (emphasis added). As noted, however, the Petition earlier stated that Peterka *already* provides unique values that are used to differentiate amongst keys, albeit in the form of *message* identifiers rather than the recited “key identifiers” of the challenged claims. Pet. 25. Once again, the Petition thus fails to articulate a reason why an ordinary

artisan would have modified Peterka to add something it does not need and to solve a problem it does not have. In particular, I note that the Petition has not demonstrated that its proposed modification would *improve* Peterka in any way compared to Peterka's *unmodified* system, particularly given the Petition's own statement that Peterka's system already provides unique message identifiers that are used to uniquely distinguish between Peterka's content keys.

96. Finally, the Petition's Ground 5 modification based on the combination of Peterka, Bocharov, Suzuki, and Peterka308—which only applies to dependent claims 7, 8 and 19—does not have sufficient a motivation. Pet. 69-73. The Petition contends that applying time stamps to Peterka's content keys as “key identifiers” would have been useful “for a client that held keys for *multiple future segments*, because it could readily compare the current playback location of a media stream to the respective location information of the future segment keys to determine which key to apply at the next key rotation boundary.” Pet. 69-70 (emphasis added). The Petition further states: “Implementing Peterka308's teaching would have beneficially allowed clients to more effectively manage keys obtained for segments *multiple periods in advance*.” Pet. 70 (emphasis added).

97. As demonstrated in detail above, however, Peterka does *not* teach providing a client with multiple content keys for “multiple future segments” or

“multiple periods in advance,” which is the premise of the Petition’s motivation for its Ground 5 modification. *See* Section IV.C., *supra*. Rather, Peterka consistently teaches providing a client *one* content key per request, and only one segment in advance. *Id.* Moreover, it would not have been obvious to modify Peterka to send clients multiple future content keys multiple segments in advance because such an approach would be contrary to Peterka’s distribution schemes. *See* ¶¶ 32-41, *supra*. Accordingly, an ordinary artisan could not have been motivated to modify Peterka in the manner proposed in Ground 5.

98. For the reasons above, the Petition thus does not meet the “key identifiers” requirement of all challenged claims on any Grounds.

VI. The Petition’s theory based on Peterka’s expiration times and pull embodiment does not meet “detecting content encryption key rotation boundaries”

A. Relevant claim language and claim interpretation

99. Claim 1 limitation [1D] recites “detecting content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content.” Claim 16 limitation [16E] contains the same requirement. The “detecting” limitation is thus required under all challenged claims.

100. The '178 Patent teaches that “[t]he transitioning between use of different keys is [] referred to herein as key ‘rotation.’” *Id.* at 1:63:65. A key rotation “boundary” occurs at the point where key rotation should occur.

101. Importantly, the '178 Patent teaches that *every* key rotation boundary can be defined through two alternative items of information provided to the client: normal-period based expiration (in which the expiration time assigned to the key is reached) and “an explicit key change notification” that requires a key change outside the period-based boundary that was otherwise defined. *Id.* at 11:3-7. (“In step 310, the client 110 checks the expiration of current content key to see if a new key should be applied. There are two cases—normal period-based expiration, and an explicit key change notification received in step 308 that applies to the current segment being decrypted.”).

102. With respect to normal period-based expiration, “the workflow manager generates content encryption keys with a fixed duration lifespan on a fixed periodic basis.” *Id.* at 3:9-11. “[T]he license server distributes fixed duration lifespan information to client.” *Id.* at 3:46-47.

103. In the context of an explicit key change notification, “a key change is signaled, i.e., a key change [is] requested outside of any fixed duration lifespan,” for instance, “for security reasons[.]” *Id.* at 10:39-43.

104. Notably, “the workflow manager may initiate content encryption key rotation at *any* time, *outside* of the fixed duration lifespan of the existing key.” *Id.* at 3:53-55 (emphasis added).

105. Because *every* “content encryption key rotation boundary” in the ’178 Patent can be defined by a notification for early, non-period-based key rotation, the client cannot reliably identify content encryption key rotation boundaries by simply monitoring the expiration time of the current key. In other words, since the next key rotation boundary in the system of the ’178 Patent may not be defined by the expiration time of the current key, the client cannot consider *only* the current key’s expiration time to correctly locate the next key rotation boundary. At the same time, the client also cannot *only* consider express key-change notifications to correctly locate key rotation boundaries, since key change notifications are not sent for all keys, and thus the appropriate boundary for a given key may be defined by its expiration time.

106. To address the fact that key rotation boundaries may be defined by *multiple* different pieces of information for any given key (expiration time and express notification), the ’178 Patent teaches “a process *for detecting the rotation of content encryption keys*.” Ex. 1001 at 9:47-49 (emphasis added). That teaching is taught entirely with respect to Figure 3, and illustrated therein. *Id.* (“FIG. 3 is a

flow chart 300 describing a process for detecting the rotation of content encryption keys and retrieving updated content encryption keys.”); Fig. 3.

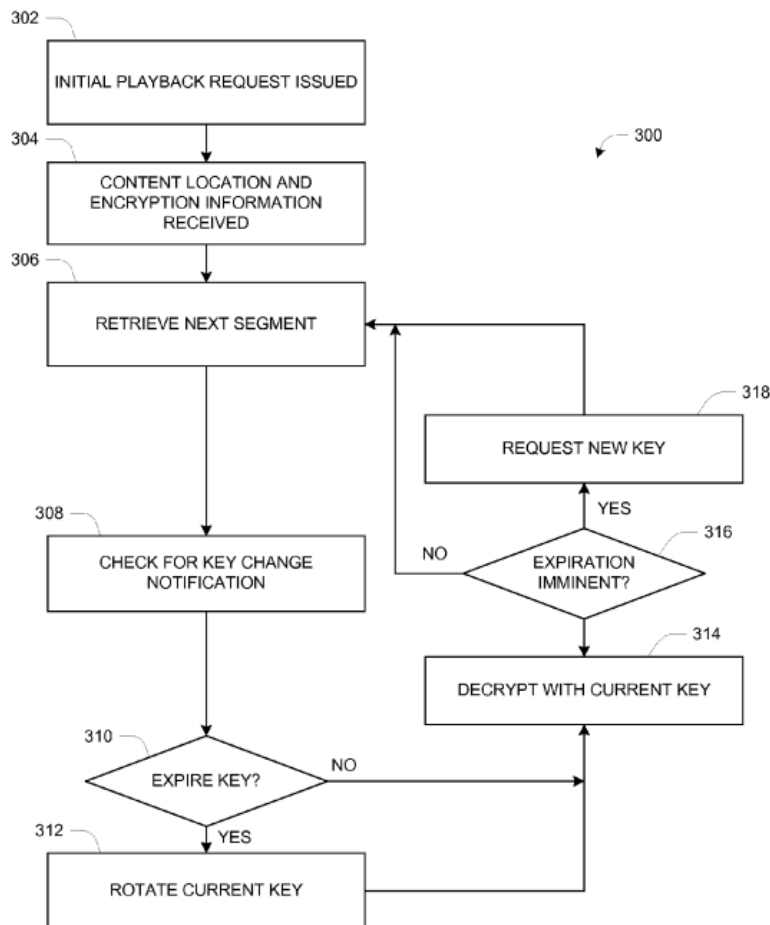


Fig. 3

107. As the '178 Patent expressly teaches in Figure 3 and the associated written description, “*detecting*” a key rotation boundary requires that the client *always* “check for key notification” at step 308. Fig. 3. The step of checking for a key change notification (step 308) as part of the overall process of “*detecting*” a key

rotation boundary is not optional, as Figure 3 illustrates. To that end, the '178 Patent teaches: "Once the new segment is retrieved, processing proceeds to step 308 where the client 110 checks to see if a key change is signaled, i.e., a key change was requested outside of any fixed duration lifespan." *Id.* at 10:39-42. The patent further teaches: "If a content encryption key change request is detected, the client notes the need to expire the current content encryption key and the content encryption key identifier of the new key to be used. The client 110 then proceeds to step 310." *Id.* at 10:65-11:2.

108. Thus, under the "process for detecting the rotation of content encryption keys" taught in the '178 Patent, *id.* at 9:47-49 (emphasis added), the client must always check for an explicit key change notification.

109. The '178 Patent further reiterates that teaching in connection with step 310 of Fig. 3: "In step 310, the client 110 checks the expiration of current content key to see if a new key should be applied. There are *two* cases—normal period-based expiration, and an explicit key change notification received in step 308 that applies to the current segment being decrypted." *Id.* at 11:2-7 (emphasis added). Once again, the '178 Patent teaches that identifying the correct rotation boundary for a current

key requires considering **both** the key's normal-period based expiration time **and** checking for "an explicit key change notification." *Id.*

110. The '178 Patent again reiterates the same two-step process in connection with step 316 of Fig. 3: "In step 316, the client 110 checks to see if the current content encryption key is going to expire in the near future **or** if a content encryption key change request for a future segment was detected in step 308. In one embodiment, when the current content encryption key is about to expire, the client 110 proactively requests a new content encryption key ahead of time to prevent any latency in or interruption of decryption services. If the current content encryption key is not close to expiring **and** a content encryption key change request was not detected in step 308, processing proceeds back to step 306 where the client 110 begins retrieving the next segment. If the current content encryption key is within a fixed threshold of expiring **or** a content encryption key change request was detected in step 308, processing proceeds to step 318 where the client 110 requests a new content encryption key from the license server 106." *Id.* at 11:38-53 (emphasis added).

111. Based on those teachings, an ordinary artisan would understand that the "**detecting**" limitation of the '178 Patent's challenged claims requires checking both a key's expiration time **and** checking for an explicit key-change notification for the

key and then identifying the applicable rotation boundary for that key in view of at least those two items of information. *Id.* at 10:39-42, 11:3-7, 11:38-41. Indeed, the '178 Patent contains no teaching in which a "rotation boundary" is "detected" *without* checking for a key change notification and considering the information provided in any such notification, and based only on consideration of an expiration time.

112. I further note that this interpretation is additionally supported by other language in the challenged claims and the testimony of Google's expert, Mr. Wechselberger. In particular, the challenged claims earlier recite "*parsing* content information from the playback request response, the content information including . . . content encryption key *expiration times*." Claim 1 limitation [1B], Claim 16 limitation [16C] (emphasis added). An ordinary artisan would have understood that once the content encryption key expiration times have been "*parsed*," the client has identified the expiration time associated with the relevant content encryption key. Google's expert Mr. Wechselberger agreed that this is what occurs. Ex. 2011 at 35:6-36:8 (Q: "In Peterka's system, once the ECMs or EMMs have been parsed to distinguish, for example, the content encryption key expiration times, does Peterka's system, at that point, know what the content key expiration times are for each key?"

A: “Yes, it will. Because Peterka explains that that information is part of what’s delivered in the ECM, along with the key.”).

113. In view of that fact, the ordinary artisan would not understand the claims’ separate requirement of “***detecting*** content encryption key rotation boundaries” to simply require identifying a key’s expiration time alone. Such an understanding would render the “detecting” limitation redundant to the “parsing” limitation, and I have been informed that claim limitations should generally not be understood as merely redundant with one another.

114. In addition, the use of the phrase “content encryption key ***rotation boundary***” in the challenged claims additionally supports my understanding that the “detecting” limitation requires more than merely monitoring or keeping track of an expiration time. The patentee clearly used “rotation boundaries” rather than “expiration times” because the change-point for the content encryption keys may be defined by express notifications in addition to by expiration times. Thus, what must be “detected” is a “rotation boundary,” not a mere expiration time, and this requires checking for both an express notification and an expiration time, analyzing the information provided as a result of that process, and then determining the appropriate rotation boundary in view of the results, as shown above. That is the “process for detecting the rotation of content encryption keys” disclosed by the ’178 Patent, Ex.

1001 at 9:47-48, and that is what the “detecting” limitation of the challenged claims requires.

B. The Petition’s expiration-time theory and Peterka’s pull embodiment do not meet the “detecting” limitation

115. To meet the “detecting” limitation, the Petition relies exclusively on Peterka’s “pull” model. Pet. 12, 18, 32-34. The Petition quotes Peterka’s teaching that, under its pull model, “each client keeps track of the keys and their *expiration times* and actively requests new keys before the current keys *expire* so as to avoid service interruptions.” Pet. 32 (quoting Ex. 1005 ¶ 105) (emphasis modified). The Petition also quotes passages from the Peterka teaching that the client will “monitor” expiration times.

116. On those bases, the Petition conclusorily states: “Peterka thus discloses clients that *detect* upcoming *content encryption key rotation boundaries* based on monitored key expiration times that allow the client to request new keys ahead of the upcoming boundary.” Pet. 32 (emphasis Petition’s). This aspect of the Petition thus contends that by simply identifying a key’s expiration time and monitoring that expiration time as part of Peterka’s pull model, Peterka discloses its clients “*detecting* content encryption key rotation boundaries.”

117. I disagree with the Petition’s expiration time theory because, as I explained in detail above, simply identifying a key’s expiration time and monitoring

that expiration time does not meet “detecting content encryption key rotation boundaries” as claimed and taught in the ’178 Patent. *See* ¶¶ 113, 114, *supra*.

118. Moreover, I note that for purposes of its “pull” model, Peterka teaches that “the server need not monitor the status of the client’s keys; rather, the responsibility of determining when a new key is required” is “passed to the client,” Ex. 1005 ¶ 106, and clients make that determination *exclusively* based on the current key’s “expiration time.” *Id.* ¶ 105 (teaching that under the “pull” model, “each client keeps track of the keys and their expiration times and actively requests new keys before the current keys *expire* so as to avoid service interruptions.”) (emphasis added). Peterka’s pull embodiment does not teach clients checking for and considering *multiple* items of information that can define the rotation boundary for a current key, and then “detecting” the appropriate rotation boundary on that basis, as the challenged claims of the ’178 Patent require.

119. Accordingly, the Petition does not and could not meet the “detecting” limitations of [1D] and [16E] based on Peterka’s “pull” embodiment.

VII. The Petition’s theory based on Peterka’s notifications does not meet the “issuing requests” requirement of all challenged claims

120. As an alternative to the expiration-time based theory, the Petition separately argues that Peterka meets the “detecting” limitation through Peterka’s teaching of signaling a key change for a content key. Pet. 33; Ex. 1005 ¶¶ 116-117.

121. Claim 1 limitation [1E], however, recites: “issuing *requests* to a license server ahead of a key rotation boundary to retrieve a second content encryption key to be used after a content encryption key rotation boundary is reached.” (emphasis added). Claim 16 limitation [16F] recites the same. As I explain below, Peterka’s signaled key change teachings do not meet the “issuing requests” requirement of the challenged claims.

122. In Peterka’s signaling embodiment, Peterka teaches that “when a new key is implemented, the implementation *will be signaled* to the clients so that the clients can begin utilizing the new content key with which they *have been provided*.” Ex. 1005 ¶ 116 (emphasis added). Peterka further reiterates that the new content key “has recently been distributed to the client.” *Id.* ¶117. Thus, *before* clients receive a content key-change signal in Peterka, they have already received the “new content key” to which they will rotate.

123. Under Peterka’s “pull” model, a client *only* requests a new key based on the *expiration time* of the current key. *Id.* ¶¶ 105-106 (“Under the pull model,

each client keeps track of the keys and their expiration times and actively requests new keys before the current keys *expire* so as to avoid service interruptions.”); (“In block 818, the key and its expiration time are distributed to the client in response to the request by the client. Thus the server need not monitor the status of the client’s keys; rather, the responsibility of determining when a new key is required can be passed to the client.”).

124. Peterka’s pull model thus does not disclose clients *requesting* a new key where a *signal* has notified the client of an upcoming content key change. To the contrary, Peterka teaches that in its signaling embodiment, the client has already “been provided” the new content key *before* the client received the key change signal. Ex. 1005 ¶¶ 116-117. Since the client could not have known that a key change signal would arrive, the client could not have issued a “pull” request for a new content key in view of the key change signal.

125. Moreover, Peterka teaches that in its pull model, clients themselves determine when a new key is required, and that “the server need not monitor the status of the client’s keys[.]” *Id.* ¶ 106. But in Peterka’s signaling embodiment, it is the server that determines when a new key is required, and the server does need to monitor the status of the client’s keys to make that determination. *Id.* ¶ 116 (“when a new content key is implemented, the implementation will be signaled to the clients

so that the clients can begin using the new content key[.]”); *id.* ¶ 117 (“a predetermined bit can be used to indicate if an old or current content key should be used as opposed to a new content key”). Peterka’s signaling method is thus incompatible with Peterka’s “pull” method.

126. Accordingly, Peterka does not teach or suggest clients “issuing requests” for a new content key under Peterka’s key-change signaling method. Rather, the new content key that Peterka has already provided to clients ahead of a signal to change keys was provided through Peterka’s push method, without clients issuing a request for that new content key. The Petition’s signaling method theory thus cannot meet limitations [1E] and [16F] of all challenged claims.

127. The Petition further contends that “signaling when to use a key in the client’s possession ***does not require*** Peterka’s server to ***push*** updated keys.” Pet. 33-34 (emphasis Petition’s). That assertion, however, does not address the fact that (1) Peterka does not teach clients “pulling” or “requesting” new content keys in the context of a signaled key change; and (2) in Peterka’s signaling method, clients receive the new content key ***before*** receiving a key change signal, and thus could not have requested or pulled the new key on that basis.

128. The Petition further argues that “using Peterka’s key change signaling with Peterka’s pull model would have been obvious.” Pet. 34. I disagree. As Mr.

Wechselberger states in connection with this obviousness theory, under Peterka’s pull model, clients only request new keys based on upcoming expiration times, *not* signaled key changes. Ex. 1003 ¶ 115. Since Peterka’s servers can signal a content key change at any time, including *before* a client has made a “pull” request for a new key based on the current key’s expiration time, combining Peterka’s pull model with its signaled key change method would expose Peterka’s clients to *not having* the necessary “new content key” that they have been signaled to use. That outcome is incompatible with Peterka’s teaching that under its signaled key change method, “when a new content key is implemented, the implementation will be signaled to clients so that the clients can begin utilizing the new content key *with which they have been provided.*” Ex. 1005 ¶ 116 (emphasis added). It is also incompatible with Peterka’s teaching that the “new content key” has “recently *been distributed* to the client.” *Id.* ¶ 117 (emphasis added). Accordingly, an ordinary artisan would not have been motivated to combine Peterka’s pull method with its signaled key change method because the combination would disconnect the relationship between when a content key should be changed, and when the client obtains the new content key,

exposing clients to lacking the next key they require, all of which is contrary to Peterka's signaled key change method teachings.

129. The Petition's reliance on Peterka's signaled key change teachings thus does not meet or render obvious the "issuing requests" limitation of all challenged claims.

* * *

130. Accordingly, the Petition does not meet or render obvious the challenged claims based on either its expiration time theory or its key change signaling theory.

VIII. Conclusion

131. For the reasons above, the challenged claims of the '178 Patent are not taught or rendered obvious by any Ground presented in the Petition.

132. I reserve the right to supplement my opinions in response to any arguments by Petitioner or its expert, and to take into account new information as it becomes available to me.

I hereby declare that all statements made herein of my own knowledge are true and that all opinions expressed herein are my own; and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed on July 2, 2025



John Villasenor, Ph.D.

EXHIBIT A

John D. Villasenor

Education

1986 – 1989	Stanford University Ph.D. in Electrical Engineering
1985 – 1986	Stanford University M.S. in Electrical Engineering
1982 – 1985	University of Virginia B.S. in Electrical Engineering

Appointments

Since 1992	University of California, Los Angeles <i>Current Position: Professor of Electrical Engineering, Law, Public Policy, and Management; Founder and Faculty Co-Director, Institute for Technology, Law, and Policy</i> Focus on innovative communications, networking, security, artificial intelligence, signal and image processing, and computing technologies and their broader implications. Have taught classes in the UCLA schools of engineering, law, public affairs, and management. See http://johnvillasenor.com for more information, including publications.	Los Angeles, CA
Since 2011	The Brookings Institution <i>Nonresident Senior Fellow, Governance Studies Program</i> Examining a broad range of issues at the intersection of technology, policy, and law, generally related to the topics listed above. See https://www.brookings.edu/experts/john-villasenor/ .	Washington, DC
2014-2023	Stanford University <i>The Hoover Institution: National Fellow (2014-2016), Visiting Fellow (2016-2018), Senior Fellow (2018-2023).</i>	Stanford, CA
1990 – 1992	Jet Propulsion Laboratory Developed new techniques for imaging and mapping the earth from space.	Pasadena, CA

Other Professional Activities

- Member, Council on Foreign Relations
- Have provided congressional testimony approximately half a dozen times (before the Senate Judiciary Committee, House Judiciary Committee, the Senate Commerce Committee, and the House Energy and Commerce Committee). See <http://johnvillasenor.com/publications/congressional-testimony/>.
- Have contributed to international standards organizations and industry consortia for the development of new communications standards.
- Served as Vice Chair of the International Center for Missing and Exploited Children's Digital Economy Task Force. See <https://tmsnrt.rs/4cKAdp6>.

- Developed and implemented an online training program covering patents, copyright, trademarks, and trade secrets. The program was adopted and implemented by the University of California system.

Patents

- Approximately 20 issued U.S. patents in areas including communications, information processing, and cybersecurity.

Publications

- Approximately 200 academic publications in technology and law journals (see below; see also <http://johnvillasenor.com>). “H-index” of 53 (as of 2024). Articles and commentary also published in broader interest venues including the *Atlantic*, *Billboard*, the *Chronicle of Higher Education*, *Fast Company*, *Forbes*, the *Huffington Post*, the *Los Angeles Times*, the *New York Times*, *Scientific American*, *Slate*, and the *Washington Post*.

Note: In the list below, engineering papers are listed first, followed by law publications.

Technical Papers Published in Academic Journals; Book Chapters

1. Jason Jaskolka and John Villasenor, “An approach for identifying and analyzing implicit interactions in distributed systems,” *IEEE Transactions on Reliability*, Vol. 66, No. 2, pp. 529-546, June 2017.
2. John Villasenor, “A probabilistic framework for modelling false Title IX ‘convictions’ under the preponderance of the evidence standard,” *Law, Probability and Risk*, Vol.15, No. 5, pp. 223-237, December 2016.
3. Lok-Won Kim and John Villasenor, “Dynamic function verification for system-on-chip security against hardware-based attacks,” *IEEE Transactions on Reliability*, Vol. 64, No. 4, pp. 1229-1242, November 2015.
4. Jerry Lien, Laura Hughes, Jorge Kina, and John Villasenor, “Mobile money solutions for a smartphone-dominated world,” *Journal of Payments Strategy & Systems*, Vol. 9, No. 3, pp. 341-350, Fall, 2015. Available at SSRN: <http://ssrn.com/abstract=2632372>
5. Lok-Won Kim and John Villasenor, “Automated iterative pipelining for ASIC design,” *ACM Transactions on Design Automation of Electronic Systems*, Vol. 20, No. 2, February 2015.
6. Lok-Won Kim and John Villasenor, “Dynamic function replacement for system-on-chip security in the presence of hardware-based attacks,” *IEEE Transactions on Reliability*, Vol. 63, No. 2, pp. 661-675, June 2014.
7. Przemyslaw Pawelczak, Shaunak Joshi, Sateesh Addepalli, John Villasenor, Danijela Cabric, “Impact of the connection admission process on the direct retry load balancing algorithm in cellular networks,” *IEEE Transactions on Mobile Computing*, Vol. 12, No. 9, pp. 1681-1696, September 2013.
8. Jianwen Chen, Jason Cong, Luminita A. Vese, John Villasenor, Ming Yan, and Yi Zou, “A hybrid architecture for compressive sensing 3D CT reconstruction,” *IEEE Journal on Emerging and Selected*

Topics in Circuits and Systems, Special Issue: Circuits, Systems and Algorithms for Compressive Sensing, Vol. 2, No. 3, pp. 616-625, Oct. 2012.

9. Jianwen Chen, Jianhua Zheng, Feng Xu, and John Villasenor, "Adaptive frequency weighting for high-performance video coding," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 22, No. 7, pp. 1027-1036, July 2012.
10. W. Hu, J. Wen, W. Wu, Y. Han, S. Yang, and J. Villasenor, "Highly scalable parallel arithmetic coding on muti-core processors using LDPC codes," IEEE Transactions on Communications, Vol. 60, No. 2, pp. 289-194, February 2012.
11. J. Chen, F. Xu, Y. He, J. Villasenor, Y. Han, Y. Xu, Y. Rong, C. Reader, and J. Wen, "Efficient video coding using legacy algorithmic approaches," IEEE Transactions on Multimedia, Vol. 14, No. 1, pp. 111-120, February, 2012.
12. D. Lee, L. Kim, and J. Villasenor, "Precision-aware, self-quantizing hardware architectures for the discrete wavelet transform," IEEE Transactions on Image Processing, Vol. 21, No. 2, pages 768-777, February 2012.
13. L.W. Kim and J.D. Villasenor, "A system-on-chip bus architecture for thwarting integrated circuit Trojan horses," IEEE Transactions on VLSI Systems, vol. 19, no. 10, pp. 1921-1926, October 2011.
14. Y. Han, J. Wen, D. Cabric and J. Villasenor, "Using a vector of observations to identify the number of frequency-hopping transmitters," IEEE Communications Letters, vol. 15, no. 3, pp. 299-301, March 2011.
15. D. Lee, H. Kim, M. Rahimi, D. Estrin, and J.D. Villasenor, "Energy-efficient image compression for resource-constrained platforms," IEEE Transactions on Image Processing, vol. 18, no. 9, pp. 2100-2113, September 2009.
16. D. Lee, R.C.C. Cheung, W. Luk, and J.D. Villasenor, "Hierarchical segmentation for hardware function evaluation," IEEE Transactions on VLSI Systems, vol. 17, No. 1, pp. 103-116, January 2009.
17. D. Lee and J.D. Villasenor, "Optimized custom precision function evaluation for embedded processors," IEEE Transactions on Computers, vol. 58, no. 1, pp. 46-59, January 2009.
18. H. Kim, M. Rahimi, D. Lee, D. Estrin, and J.D. Villasenor, "Energy-aware high resolution image acquisition via heterogeneous image sensors," IEEE Journal of Selected Topics in Signal Processing, vol. 2, no. 4, pp. 526-537, August 2008.
19. H. Kim, D. Lee, and J.D. Villasenor, "Design tradeoffs and hardware architecture for real-time iterative MIMO detection using sphere decoding and LDPC coding," IEEE Journal on Selected Areas in Communications, vol. 26, no. 6, pp. 1003-1014, August 2008.
20. D. Choi, K. Choi, and J.D. Villasenor, "New non-volatile memory structures for FPGA architectures," IEEE Transactions on VLSI Systems, vol. 16, no. 7, pp. 874-881, July 2008.
21. H. Kim and J.D. Villasenor, "Secure MIMO communications in a system with equal numbers of transmit and receive antennas," IEEE Communications Letters, vol. 12, no. 5, pp. 386-388, May 2008.

22. D. Lee, H. Kim, C. Jones, and J.D. Villasenor, "Pilotless frame synchronization for LDPC-coded transmission systems," *IEEE Transactions on Signal Processing*, vol. 56, No. 7, pp. 2865 - 2874, July 2008.
23. D. Lee, R.C.C. Cheung, J.D. Villasenor, and W. Luk, "Hardware implementation tradeoffs of polynomial approximations and interpolations," *IEEE Transactions on Computers*, vol. 57, no. 5, pp. 686-701, May 2008.
24. D.B. Thomas, W. Luk, P.H.W. Leong, and J.D. Villasenor, "Gaussian random number generators," *ACM Computing Surveys*, vol. 39, issue 4, article 11, October 2007.
25. D. Lee, H. Kim, C.R. Jones, and J.D. Villasenor, "Pilotless frame synchronization via LDPC code constraint feedback," *IEEE Communications Letters*, vol. 11, no. 8, pp. 683-685, August 2007.
26. R.C.C. Cheung, D. Lee, W. Luk, and J.D. Villasenor, "Hardware generation of arbitrary random number distributions from uniform distributions via the inversion method," *IEEE Transactions on VLSI Systems*, vol. 15, no. 8, pp. 952-962, August 2007.
27. H. Kim, J. Wen, and J.D. Villasenor, "Secure arithmetic coding," *IEEE Transactions on Signal Processing*, vol. 55, no. 5, pp. 2263 - 2272, May 2007.
28. D. Lee, R.C.C. Cheung, and J.D. Villasenor, "A flexible architecture for precise gamma correction," *IEEE Transactions on VLSI Systems*, vol. 15, no. 4, pp. 474-479, April 2007.
29. D. Lee and J.D. Villasenor, "A bit-width optimization methodology for polynomial-based function evaluation," *IEEE Transactions on Computers*, vol. 56, no. 4, pp. 567-571, April 2007.
30. C. Jones, T. Tian, J.D. Villasenor, and R. Wesel, "The universal operation of LDPC codes over scalar fading channels," *IEEE Transactions on Communications*, vol. 55, no. 1, pp.122-132, January 2007.
31. M.D. Smith and J. Villasenor, "JPEG-2000 rate control for digital cinema," *SMPTE Motion Imaging Journal*, vol. 115, no. 10, pp. 394-399, October 2006.
32. D. Lee, J.D. Villasenor, W. Luk and P.H.W. Leong, "A hardware Gaussian noise generator using the Box-Muller method and its error analysis," *IEEE Transactions on Computers*, vol. 55, no. 6, pp. 659-671, June 2006.
33. D. Lee, E.L. Valles, J.D. Villasenor and C.R. Jones, "Joint LDPC decoding and timing recovery using code constraint feedback," *IEEE Communications Letters*, vol. 10, no. 3, pp. 189-191, March 2006.
34. J. Wen, H. Kim and J.D. Villasenor, "Binary arithmetic coding with key-based interval splitting," *IEEE Signal Processing Letters*, vol. 13, No. 2, pp. 69-72, February 2006.
35. William J. Kaiser, Gregory J. Pottie, Mani Srivastava, Gaurav S. Sukhatme, John Villasenor, and Deborah Estrin, *Networked infomechanical systems (NIMS) for ambient intelligence*. Weber W, Rabaey JM, eds. *Ambient Intelligence* (Springer, Berlin), 83–113, 2005.
36. D. Lee, W. Luk, J.D. Villasenor, G. Zhang and P.H.W. Leong, "A hardware Gaussian noise generator using the Wallace method," *IEEE Transactions on VLSI Systems*, vol. 13, no. 8, pp. 911-920, August 2005.

37. P.H.W. Leong, G. Zhang, D. Lee, W. Luk and J.D. Villasenor, "A comment on the implementation of the zigurat method," *Journal of Statistical Software*, vol. 12, no. 7, February 2005.
38. D. Lee, W. Luk, J.D. Villasenor and P.Y.K Cheung, "A Gaussian noise generator for hardware-based simulations," *IEEE Transactions on Computers*, vol. 53, no. 12, pp. 1523-1534, December 2004.
39. D. Lee, W. Luk, J.D. Villasenor and P.Y.K Cheung, "The effects of polynomial degrees on the hierarchical segmentation method," in *New Algorithms, Architectures, and Applications for Reconfigurable Computing*, Chapter 24, W. Rosenstiel and P. Lysaght (Eds.), Springer-Verlag, December 2004.
40. T. Tian, C. Jones, J.D. Villasenor, and R. Wesel, "Selective avoidance of cycles in irregular LDPC code construction," *IEEE Transactions on Communications*, vol. 52, no. 8, pp. 1242-1247, August 2004.
41. "Networked Infomechanical Systems (NIMS) for Ambient Intelligence", CENS Technical Report 31, December 2003 (PDF File). Ambient Intelligence, J. Rabaey et. Al., 2004
42. K. Lakovic, J. Villasenor, "An algorithm for construction of efficient fix-free codes," *IEEE Communication Letters*, vol. 7, no. 8, pp. 391-393, August 2003.
43. J. Garcia-Frias, J.D. Villasenor, "Combined turbo detection and decoding for unknown ISI channels", *IEEE Transactions on Communications*, vol. 51, no. 1, pp. 79-85, January 2003.
44. K. Lakovic, J. Villasenor, "On the design of error-correcting reversible variable length codes," *IEEE Communication Letters*, vol. 6, no. 8, pp. 337-339, August 2002.
45. Jiangtao Wen and J.D. Villasenor, "Soft-input soft-output decoding of variable length codes," *IEEE Transactions on Communications*, vol. 50, No. 5, pp. 689-692, May 2002.
46. J. Garcia-Frias and J.D. Villasenor, "Turbo decoding of Gilbert-Elliot channels," *IEEE Transactions on Communications*, vol. 50, no.3, pp. 357-363, March 2002.
47. J. Garcia-Frias and J.D. Villasenor, "Joint turbo decoding and estimation of hidden Markov sources," *IEEE Journal on Selected Areas in Communications*, vol. 19, no. 9, pp. 1671-1679, September 2001.
48. S. Saha, M. Jamtgaard and J.D. Villasenor, "Bringing the wireless internet to mobile devices," *Computer*, vol. 34, no.6, pp.54-58, June 2001.
49. D. Lau, A. Schneider, M.D. Ercegovac and J.D. Villasenor "An FPGA-based library for on-line signal processing," *Journal of VLSI Signal Processing Systems for Signal, Image, and Video Technology*, vol. 28, no. 1-2, pp. 129-143, May-June 2000.
50. J. Wen, M.Luttrell and J.D Villasenor, "Trellis-based R-D optimal quantization in H.263+," *IEEE Transactions on Image Processing*, vol. 9, no. 8, pp. 1431-1434, Aug. 2000.
51. J.Y. Liao and J.D. Villasenor, "Adaptive intra block update for robust transmission of H.263," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 10, no. 1, pp. 30-35, February 2000.

52. J.D. Villasenor, Y.Q. Zhang, and J. Wen, "Robust video coding algorithms and systems," Proceedings of the IEEE, vol. 87, no. 10, pp. 1724-1733, October 1999.
53. J. Wen and J.D. Villasenor, "Structured prefix codes for quantized low-shape-parameters generalized Gaussian sources," IEEE Transactions on Information Theory, vol. 45, no. 4, pp. 1307-1314, May 1999.
54. J. Garcia-Frias and J.D. Villasenor, "Turbo decoders for Markov channels," IEEE Communications Letters, vol. 2, no. 9, pp. 257-259, September 1998.
55. John Villasenor and Brad Hutchings, "The flexibility of configurable computing," IEEE Signal Processing Magazine, vol. 15, no. 5, pp. 67-84, September 1998.
56. Kang-Ngee Chia, Hea Joung Kim, Shane Lansing, William Mangione-Smith, and John Villasenor, "High-performance automatic target recognition through data-specific VLSI," IEEE Transactions on Very Large Scale Integration Systems, vol. 6, no. 3, pp. 364-371, September 1998.
57. Niko Faerber, Bernd Girod, and John Villasenor, "Extensions of ITU-T Recommendation H.324 for error-resilient video transmission," IEEE Communications Magazine, vol. 36, pp. 120-128, June 1998.
58. B. Belzer and J.D. Villasenor, "Symmetric trellis coded vector quantization," IEEE Transactions on Communications, vol. 45, no. 11, pp. 1354-1357, November 1997.
59. A. Watson, G. Yang, J. Solomon, and J.D. Villasenor, "Visibility of wavelet quantization noise," IEEE Transactions on Image Processing, vol. 6, no.8, pp 1164-1175, August 1997.
60. J. Garcia-Frias and J.D. Villasenor, "Combining hidden Markov source models and parallel concatenated codes," IEEE Communications Letters, vol. 1, no. 4, pp. 111-113, July 1997.
61. A. Lientz and J.D. Villasenor, "Very low variable rate convolutional codes for unequal error protection in DS-CDMA systems," IEEE Transactions on Communications, vol. 45, no. 7, pp. 753-755, July 1997.
62. John Villasenor and William H. Mangione-Smith, "Configurable computing," Scientific American, pp. 66-71, June 1997. (Strictly speaking, this publication is not in a traditional academic journal. However, I am including it here because it is technical in nature and has been very widely cited in the academic literature.)
63. F. Chen, Z. Gao, and J.D. Villasenor, "Lattice Vector quantization of Generalized gaussian sources," IEEE Transactions on Information Theory, vol. 43, pp. 92-103, January 1997.
64. M.J. Tsai, J.D. Villasenor, and F. Chen, "Stack-run image coding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 6, pp. 519-521, October 1996.
65. A. Alwan, R. Bagrodia, N. Bamos, M. Gerla, L. Kleinrock, J. Short, J.D Villasenor, "Adaptive mobile multimedia networks," IEEE Personal Communications, vol. 3, no. 2, pp. 34-51, April 1996.
66. J.D. Villasenor, C. Jones, and B. Schoner, "Video communications using rapidly reconfigurable hardware," IEEE Transactions on Circuits and Systems for Video Technology, vol. 5, pp. 565-567, December 1995.

67. Z. Gao, F. Chen, B. Belzer, and J.D. Villasenor, "A comparison of the Z, E8, and Leech lattices for quantization of low-shape-parameter generalized Gaussian sources," *IEEE Signal Processing Letters*, vol. 2, pp. 197-199, October 1995.
68. J.D. Villasenor, B. Belzer, J. Liao, "Wavelet filter evaluation for image compression," *IEEE Transactions on Image Processing*, vol. 4, no. 8, pp. 1053-1060, August 1995.
69. J.D. Villasenor, "Tomographic image compression using multidimensional transforms," *The Journal of Information Processing and Management*, vol. 30, no. 8 pp. 817-824, November 1994.
70. J.D. Villasenor, "Optical Hartley transforms," *Proceedings of the IEEE*, vol. 82, no. 3, pp. 391-399, March 1994.
71. A. Freeman, J.D. Villasenor, J.D. Klein, P. Hoogeboom, and J. Groot, "On the use of multi-frequency and polarimetric radar backscatter features for classification of agricultural crops," *International Journal of Remote Sensing*, vol. 15, no. 9, pp. 1799-1812, 1994.
72. J.D. Villasenor, "Alternatives to the Discrete Cosine Transform for irreversible tomographic image compression," *IEEE Transactions on Medical Imaging*, vol. 12, no. 4, pp. 803-812, December 1993.
73. H.A. Zebker and J.D. Villasenor, "Decorrelation in interferometric radar echoes," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 30, no. 5, pp. 950-959, September 1992.
74. John Villasenor and Alain Vincent, "An algorithm for space recognition and time tracking of vorticity tubes in turbulence," *CVGIP: Image Understanding*, vol. 55, No. 1, pp. 27-25, January 1992.
75. John Villasenor and Oscar Buneman, "Rigorous charge conservation for local electromagnetic field solvers," *Computer Physics Communications*, vol. 69, no. 2, pp. 306-316, March 1992.
76. S.C. Pei, S.B. Jaw, J.D. Villasenor, and R.N. Bracewell, "Comment on 'Vector Hartley transform'," *Electronics Letters*, vol. 26, no. 2, pp. 94-95, January 1990.
77. R.N. Bracewell and J.D. Villasenor, "Fraunhofer diffraction by a spiral slit," *Journal of the Optical Society of America*, vol. 7, no. 1, pp. 21-25, 1990.
78. J.D. Villasenor and R.N. Bracewell, "Lensless microwave imaging using the Hartley transform," *Nature*, vol. 335, pp. 617-619, October 1988.
79. John Villasenor, "Two-dimensional optical Hartley transforms in the presence of errors," *Applied Optics*, vol. 28, no. 13, pp. 2671-2676, 1989.
80. J.D. Villasenor and R.N. Bracewell, "Vector Hartley transform," *Electronics Letters*, vol. 25, no. 17, pp. 1110-1111, August 1989.
81. John Villasenor and R.N. Bracewell, "Optical phase obtained by analogue Hartley transformation," *Nature*, vol. 330, pp. 735-737, December 1987.
82. R.N. Bracewell, O. Buneman, H. Hao, and J.D. Villasenor, "Fast two-dimensional Hartley transform," *Proceedings of the IEEE*, vol. 74, no. 9, pp. 1282-1283, September 1986.

Technical Conference Papers

83. Pratyush Garg, John Villasenor & Virginia Foggo, "Fairness Metrics: A Comparative Analysis," Proceedings of the IEEE International Conference on Big Data, December 2020.
84. Jason Jaskolka and John Villasenor, "Identifying Implicit Component Interactions in Distributed Cyber-Physical Systems," Proceedings of HICSS-50 (Hawaii International Conference on System Sciences), Honolulu, HI, Jan. 2017.
85. Jianwen Chen, Feng Xu, John Villasenor, Tao Fan, Haiwu Zhao, Guozhong Wang, "An adaptive covariance-based edge diffusion image enlargement method," Proceedings of the Visual Communications and Image Processing (VCIP) 2012, San Diego, CA, Nov. 2012.
86. J. Villasenor, Y. Han, D. Wen, E. Gonzalez, and J. Chen, "The information rate of modern speech and its implications for language evolution," Proceedings of the Ninth Evolution of Language Conference (Evolang), Kyoto, Japan, pp. 376-383, March 2012.
87. P. Monajemi, R. Sahasrabudhe, and J. Villasenor, "Scheduling in heterogeneous cellular networks with mobility," 2012 Information Theory and Applications Workshop, San Diego, February 2012.
88. M. Yan, J. Chen, L. A. Vese, J. Villasenor, A. Bui and J. Cong, "EM+TV based reconstruction for cone-beam CT with reduced radiation," Proceedings of the 7th International Symposium on Visual Computing (ISVC), Part I, LNCS 6938, pp. 1-10, Las Vegas, Nevada, Sept. 2011.
89. Jianwen Chen, Ming Yan, Luminita Vese, John Villasenor, Alex Bui, and Jason Cong, "EM-TV for reconstruction of cone-beam CT with curved Detectors using GPU," Proceedings of the Fully Three-Dimensional Image Reconstruction in Radiology and Nuclear Medicine Conference, pp. 363-366, July, 2011.
90. Xinyu Zhang, Zhuoyuan Chen, Jiangtao Wen, Jianwei Ma, Yuxing Han and John Villasenor, "A compressive sensing reconstruction algorithm for trinary and binary sparse signals using pre-mapping," Proceedings of the 2011 IEEE Data Compression Conference (DCC), March, 2011.
91. Xinyu Zhang, Jiangtao Wen, Yuxing Han and John Villasenor, "An improved compressive sensing reconstruction algorithm using linear/non-linear mapping," Proceedings of the Information Theory and Application Workshop (ITA), San Diego, February, 2011.
92. Esteban Valles, Richard Wesel, John Villasenor, Christopher Jones, and Marvin Simon, "Pilotless carrier phase-synchronization via LDPC code feedback," Proceedings of Milcom 2010, October 2010.
93. Shaunak Joshi, Przemyslaw Pawelczak, Sateesh Addepalli, John Villasenor, and Danijela Cabric, "Connection Admission Versus Load Balancing," Proceedings of IEEE Globecom 2010, Miami, December 2010.
94. Y. K. Jang and J. Villasenor, "SINR improvement through reconfigurable antenna adaptation to handheld device orientation," Proceedings of the IEEE AP-S International Symposium, Toronto, Canada, July 2010.
95. Yuxing Han, Jiangtao Wen, Danijela Cabric, Sateesh Addepalli, John Villasenor, "A probabilistic approach to identifying the number of transmitters in the presence of mis-detection," Proceedings of the 2010 IEEE Int. Conference on Communications (ICC), Cape Town, South Africa, June 2010.

96. Jiangtao Wen, Zhuoyuan Chen, Yuxing Han, John Villasenor, and Shiqiang Yang, "Reconstruction of sparse binary signals using compressive sensing," Proceedings of the 2010 IEEE Data Compression Conference, March, 2010.
97. Zhuoyuan Chen, Jiangtao Wen, Yuxing Han, John Villasenor, and Shiqiang Yang, "Image compression using the DCT and noiselets: a new algorithm and its rate distortion performance," Proceedings of the 2010 IEEE Data Compression Conference, March, 2010.
98. Zhuoyuan Chen, Jiangtao Wen, Yuxing Han, John Villasenor, Shiqiang Yang, "A compressive sensing image compression algorithm using quantized DCT and noiselet information," Proceedings of IEEE ICASSP 2010, Dallas, March 2010.
99. Yuxing Han, Shaunak Joshi, Lillian Dai, Danijela Cabric, Sateesh Addepalli, Jiangtao Wen and John Villasenor, "A Probabilistic Approach to Identifying the Number of Frequency Hoppers for Spectrum Sensing," Proceedings of Globecom 2009, Dec. 2009.
100. Shaunak Joshi, Ray C.C. Cheung, Pooya Monajemi, and John Villasenor, "Traffic-based study of femtocell access policy impacts on HSPA service quality," Proceedings of Globecom 2009, Dec. 2009.
101. Lok-Won Kim, John D. Villasenor and Cetin K. Koc, "A Trojan-resistant system-on-chip bus architecture," Proceedings of IEEE Military Communication (MILCOM) 2009, Boston, Oct. 2009.
102. Alican Gok, Shaunak Joshi, John Villasenor and Danijela Cabric, "Estimating the Number of Bluetooth Transmitters Using Spectral Sensing With Time and Frequency Offset Measurements," Proceedings of IEEE Military Communication (MILCOM) 2009, Boston, Oct. 2009.
103. Ray C.C. Cheung, C.K. Koc, and John Villasenor, "An efficient hardware architecture for spectral hash algorithm," Proceedings of the IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP), Boston, July 7 -9, 2009.
104. K. Soroushian, S. Priyadarshi, and J. Villasenor, "H.264 parameter optimizations for internet based distribution of high quality video," Proceedings of the SMPTE 2008 Annual Technical Conference, October 2008.
105. S. Priyadarshi, K. Soroushian and J. Villasenor, "Rich metadata description for interactivity and dynamic user-generated information," Proceedings of the SMPTE 2008 Annual Technical Conference, October 2008.
106. D. Choi, P. Monajemi, S. Kang, and J. Villasenor, "Dealing with loud neighbors: the benefits and tradeoffs of adaptive femtocell access," Proceedings of Globecom 2008, December 2008.
107. Yuxing Han, Jiangtao Wen and John D. Villasenor, "Entropy coding using equiprobable partitioning," Proceedings of the Forty-Sixth Annual Allerton Conference on Communication, Control, and Computing, September 2008.
108. M.D. Smith and J.D. Villasenor, "Bitrate Reduction Techniques for Stereoscopic Digital Cinema Distribution," SPIE Electronic Imaging Conference 2008: Visual Communications and Image Processing (VCIP), vol. 6822, pp. 1-9, San Jose, CA, January 2008.

109. D. Lee, H. Kim, S. Tu, M. Rahimi, D. Estrin, and J.D. Villasenor, "Energy-optimized image communication on resource-constrained sensor platforms," Proceedings of the IEEE/ACM International Conference on Information Processing in Sensor Networks: Special Track on Sensor Platforms, Tools and Design Methods (SPOTS), pp. 126-225, Cambridge, MA, Apr 2007.
110. M.D. Smith and J. Villasenor, "Constant Quality JPEG2000 Rate Control for Digital Cinema," Proceedings of the Visual Communication and Image Processing Conference, VCIP 2007, San Jose, CA, Jan 2007.
111. D. Lee, R.C.C. Cheung, J.D. Villasenor and W. Luk, "Inversion-based hardware Gaussian random number generator: a case study of function evaluation via hierarchical segmentation," Proceedings of the IEEE International Conference on Field-Programmable Technology (FPT), pp. 33-40, Bangkok, Thailand, Dec 2006.
112. R. Osborne and J. Villasenor, "Video traffic modeling for resource-constrained clients," Proceedings of Globecom 2006, Nov 2006. E. Valles, C. Jones, J. Villasenor, and R. Wesel, "Carrier and timing synchronization of BPSK via LDPC code feedback," Proceedings of the 40th Annual Asilomar Conference on Signals, Systems, and Computers, pp. 2177-2181, Pacific Grove, CA, Nov 2006.
113. Marvin Simon, Esteban Valles, Christopher Jones, Richard Wesel and John Villasenor, "Information-reduced carrier synchronization of BPSK and QPSK using soft decision feedback," Proceedings of the 44th Annual Allerton Conference on Communications, Control and Computing, September 2006.
114. D. Choi, E.P. Kwon, H. Lee, J. Chang, K. Choi, and J. Villasenor, "Single-chip integration of SRAM and non-volatile memory using bit-line sharing," Proceedings of the European Solid State Circuits Conference (ESSCIRC) 2006, pp. 295-298, Sept 2006.
115. K. Lakovic, T. Tian, and J. Villasenor, "Iterative Decoder design for joint source-Channel LDPC coding," Proceedings of IEEE EUROCON 2005, pp. 486-489, Nov. 2005.
116. E. Valles, A.I. Vila Casado, M. Blaum, J. Villasenor, and R.D. Wesel, "Hamming codes are rate-efficient array codes," Proceedings of the Globecom 2005, vol. 3, pp. 1320-1324, December 2005.
117. J. Wen, H. Kim and J.D. Villasenor, "Secure arithmetic coding using interval splitting," Proceedings of the 39th Annual Asilomar Conference on Signals, Systems, and Computers, pp. 1218-1221, Pacific Grove, CA, October 2005.
118. G. Zhang, P.H.W. Leong, D. Lee, J.D. Villasenor, R.C.C. Cheung, and W. Luk, "Zigurat-based hardware Gaussian random number generator," Proceedings of the IEEE International Conference on Field Programmable Logic and its Applications (FPL), Tampere, Finland, September 2005.
119. M. Smith, J. Villasenor, "Intra-frame JPEG-2000 vs. inter-frame compression comparison: The benefits and trade-offs for very high quality, high resolution sequences," Proceedings of the SMPTE Technical Conference and Exhibition, pp. 1-9, Pasadena, CA., October 2004.
120. T. Tian, C. Jones, and J. Villasenor, "Rate-compatible low-density parity-check codes," Proceedings of the International Symposium on Information Theory, Chicago, IL, July 2004.

121. D. Lee, W. Luk, C. Wang, C. Jones, M. Smith and J.D. Villasenor, "A flexible hardware encoder for low-density parity-check codes," Proceedings of the IEEE Symposium on Field-Programmable Custom Computing Machines, pp. 101-111, Napa, CA, April 2004.
122. D. Lee, W. Luk, J.D. Villasenor and P.Y.K Cheung, "Hierarchical segmentation schemes for function evaluation," Proceedings of the IEEE International Conference on Field-Programmable Technology, pp. 92-99, Tokyo, Japan, December 2003.
123. C. Jones, A. Matache, T. Tian, J. Villasenor, and R. Wesel, "The Universality of LDPC Codes on wireless channels," Proceedings of the 2003 IEEE Military Communications Conference, vol. 1, pp. 440-445, October 2003.
124. C. Jones, E. Valles, M. Smith, J. Villasenor, "Approximate-MIN constraint node updating for LDPC code decoding," Proceedings of the IEEE Military Communications Conference, vol. 1 pp. 157-162, October 2003.
125. D. Lee, W. Luk, J.D. Villasenor and P.Y.K Cheung, "Non uniform segmentation for hardware function evaluation," Proceedings of the International Conference on Field Programmable Logic and Applications, Lisbon, Portugal, pp. 796-807, September 2003.
126. D. Lee, W. Luk, J.D. Villasenor and P.Y.K Cheung, "A hardware Gaussian noise generator for channel code evaluation," Proceedings of IEEE Symposium on Field-Programmable Custom Computing Machines, pp. 69-78, Napa, CA, April 2003.
127. T. Tian, C. Jones, John Villasenor, and Rick Wesel, "Construction of irregular LDPC codes with low error floors," Proceedings of the IEEE International Conference on Communications, May 2003.
128. K. Lakovic K. and J. Villasenor, "Design considerations for efficient reversible variable length codes," Proceedings of the Thirty-Sixth Asilomar Conference on Signals, Systems and Computers, pp. 262-266, Monterey, CA, November 2002.
129. C. Jones, T. Tian, Adina Matache, R. Wesel, and J. Villasenor, "Robustness of LDPC Codes in periodic fading channels," Proceedings of IEEE Globecom, Taipei, Taiwan, November 2002.
130. K. Lakovic and J. Villasenor, "On reversible variable length codes with turbo codes, and iterative source-channel decoding," Proceedings of the IEEE International Symposium on Information Theory, July 2002.
131. K. Lakovic and J. Villasenor, "Combining Variable Length Codes and Turbo Codes," Proceedings of the IEEE VTS 55th Vehicular Technology Conference, Birmingham, Alabama, May 2002.
132. Adam H. Li, Jay Fahlen, Tao Tian, Luciano Bononi, So-Young Kim, Jeong-Hoon Park, and John Villasenor, "Generic uneven level protection algorithm for multimedia data transmission over packet-switched networks," Proceedings of the IEEE International Conference on Computer Communications and Networks Proceedings, pp. 340-346, October 2001.
133. Ksenija Lakovic and John Villasenor, "Parallel concatenated codes for iterative source-channel decoding," Proceedings of the 39th Annual Allerton Conference on Communications, Control and Computing, October 2001.

134. T. Tian, A.H. Li, J.Wen and J.Villasenor, "priority dropping in network transmission of scalable video," Proceedings of the 7th IEEE International Conference on Image Processing, vol.3, pp. 400-403, Vancouver, BC, Canada, September 2000.
135. M. Luttrell, J.Wen and J. Villasenor, "Trellis-based R-D optimal quantization in H.263+," Proceedings of the 7th IEEE International Conference on Image Processing, vol.3, pp.852-854, , Vancouver, BC, Canada, September 2000.
136. Ksenija Lakovic, Christopher Jones, and John Villasenor, "Investigating Quasi Error Free (QEF) operation with turbo codes," Proceedings of the 2nd International Symposium on Turbo Codes and Related Topics, Brest, France, September 2000.
137. J. Garcia-Frias and J.D. Villasenor, "Low complexity turbo decoding for binary hidden Markov channels," Proceedings of the 2000 IEEE 51st Vehicular Technology Conference, pp. 840-843, Tokyo, Japan, May 2000.
138. Adam H. Li, Surin Kittitornkun, Yu-Hen Hu, Dong-Seek Park, and John Villasenor, "Data partitioning and reversible variable length codes for robust video communications," IEEE Data Compression Conference Proceedings, pp.460-469, March 2000.
139. Ksenija Lakovic, John Villasenor, Rick Wesel, "Robust joint Huffman and convolutional decoding," Proceedings of the IEEE VTS 50th Vehicular Technology Conference, pp. 2551-2555, Amsterdam, The Netherlands, September 1999.
140. M. Luttrell, J. Villasenor, J.H. Park, and D.S. Park, "A data partitioning based video coding algorithm for error prone channels," Proceedings of the International Packet Video Workshop 1999.
141. J. Garcia-Frias and J. Villasenor, "Combined blind equalization and turbo decoding," Proceedings of the 1999 International Communications Conference, Vancouver, Canada, June 1999.
142. J. Garcia-Frias and J. Villasenor, "Blind turbo decoding and equalization," Proceedings of the 1999 Vehicular Technology Conference, Houston, Texas, May 1999.
143. Jiangtao Wen and John Villasenor, "Utilizing soft information in decoding of variable length codes," Proceedings of the IEEE Data Compression Conference, pp. 131-139, March 1999.
144. J. Garcia-Frias and J. Villasenor, "Exploiting binary Markov channels with unknown parameters in turbo coding," Proceedings of the 1998 IEEE Global Telecommunications Conference, pp. 3244-3249, Sydney, Australia, November 1998.
145. P. Meshkat and J. Villasenor, "New schedules for information processing in turbo decoding algorithms," Proceedings of the 1998 IEEE International Symposium on Information Theory, p. 118, Cambridge, Massachusettes August 1998.
146. P. Meshkat and J. Villasenor, "Generalized versions turbo decoding in the framework of bayesian networks and pearl's belief propagation algorithm," Proceedings of the IEEE 1998 International Conference on Communications, pp. 121-125, Atlanta, Georgia, June 1998.
147. J. Garcia-Frias and J. Villasenor, "Turbo codes for binary markov channels," Proceedings of the IEEE 1998 International Conference on Communications, pp. 110-115, Atlanta, Georgia, June 1998.

148. J. Garcia-Frias and J. Villasenor, "Turbo decoding of hidden markov sources with unknown parameters," Proceedings of the 1998 IEEE Data Compression Conference, pp. 159-168, Snowbird, Utah, March 1998.
149. Jiangtao Wen and John Villasenor, "Reversible variable length codes for efficient and robust image and video coding," Proceedings of the IEEE 1998 Data Compression Conference, pp. 471-480, Snowbird, Utah, March 1998.
150. J. Garcia-Frias and J. Villasenor, "Markov structures in turbo decoding," Proceedings of the 1998 Information Theory Workshop, pp. 54-55, San Diego, California, February 1998.
151. J. Wen and J. Villasenor, "A class of reversible variable length codes for robust image and video coding," Proceedings of the IEEE International Conference on Image Processing, vol. 2, pp. 65-68, Santa Barbara, CA, October 1997.
152. J. Garcia-Frias, D. Benyamin, and J. Villasenor, "Rate-distortion optimal parameter choice in a wavelet image communications system," Proceedings of the IEEE International Conference on Image Processing, vol. 2, pp. 25-28, Santa Barbara, CA, October 1997.
153. J. Garcia-Frias and J. Villasenor, "Joint source channel decoding of turbo codes," Proceedings of the 1997 International Symposium on Turbo Codes, pp. 259-262, Brest, France, September 1997.
154. J. Garcia-Frias and J. Villasenor, "An analytical treatment of channel-induced distortion in run length coded subbands," Proceedings of the IEEE 1997 Data Compression Conference, pp. 52-61, Snowbird, Utah, March 1997.
155. A.B. Watson, G.Y. Yang, J.A. Solomon, J. Villasenor, "Visual thresholds for wavelet quantization error," Proceedings of the SPIE - The International Society for Optical Engineering, vol. 2657, pp. 382-392, 1996.
156. J. Wen, P. Meshkat, and J. Villasenor, "Structured trees for lossless coding of quantized wavelet coefficients," Proceedings of the 30th Asilomar Conference on Signals, Systems, & Computers, vol. 2, pp 931-937, Pacific Grove, CA, November 1996.
157. M.J. Tsai, J. Villasenor, and F. Chen, "Stack-run coding for low bit rate image communication," Proceedings of the 1996 IEEE International Conference on Image Processing, vol. 1, pp. 681-684, Lausanne, Switzerland, September 1996.
158. F. Chen, J. Villasenor and D.S. Park, "A low-complexity rate-distortion model for motion estimation in H.263," Proceedings of the 1996 IEEE International Conference on Image Processing, vol. 2, pp. 517-520, Lausanne, Switzerland, September 1996.
159. J.Y. Liao and J. Villasenor, "Adaptive Intra update for video coding under noisy channels," Proceedings of the 1996 International Conference of Image Processing, vol. 3, pp. 763-766, Lausanne, Switzerland, September 1996.
160. J. Villasenor, B. Schoner, K.N. Chia, and C. Zapata, H.J. Kim, C. Jones, S. Lansing, and B. Mangione-Smith, "Configurable computing solutions for automatic target recognition," Proceedings of the IEEE Symposium of FPGAs for Custom Computing Machines, pp. 70-79, Napa, CA, April 1996.

161. J. Villasenor, R.A. Ergas, and P.L. Donoho, "Seismic data compression using high-dimensional wavelet transforms," Proceedings of the IEEE 1996 Data Compression Conference, pp. 396-405, Snowbird, Utah, April 1996.
162. B. Belzer and J. Villasenor, "Symmetric trellis coded vector quantization," Proceedings of the IEEE 1996 Data Compression Conference, pp. 13-22, Snowbird, Utah, April 1996.
163. J. Villasenor, "Image compression for defense applications--perspectives and directions," Proceedings of the 1995 IEEE Military Communications Conference, Los Angeles, California, November 1995.
164. P.L. Donoho, R.A. Ergas, and J. Villasenor, "High performance seismic trace compression," Proceedings of the 65th Society of Exploration Geophysicists Conference, pp. 160-163, Houston, Texas, October 1995.
165. Benjamin Belzer, J. Villasenor, and Bernd Girod, "Joint source channel coding of images with trellis coded quantization and convolutional codes," Proceedings of the 1995 IEEE International Conference on Image Processing, vol. 2, pp. 85-88, Oct. 1995.
166. F. Chen, Z. Gao, and J. Villasenor, "A lattice vector quantizer for generalized Gaussian sources," Proceedings of the IEEE Conference on Image Processing, pp. 105-108, Oct. 23-26, 1995.
167. M.J. Tsai, J.D. Villasenor, A. Chatziioannou, and M. Dahlbom, "Positron emission tomograph compression by using wavelet transforms," Proceedings of the IEEE 1995 Nuclear Science Symposium and Medical Imaging Conference, Medical Imaging, Paper No. 7M10, , San Francisco, CA, October 1995.
168. R. Jain, J. Short, S. Nazareth, L. Kleinrock, and J. Villasenor, "PC-notebook-based mobile networking: algorithms, architectures, and implementation," Proceedings of the IEEE 1995 International Communications Conference, Seattle, Washington, June 1995.
169. B. Schoner, C. Jones and J. Villasenor, "Issues in wireless video coding using run-time-reconfigurable FPGAs," Proceedings of the IEEE Symposium on FPGAs for Custom Computing Machines, pp. 85-89, Napa, California, April 1995.
170. J. Villasenor, R. Jain, B. Belzer, W. Boring, and C. Jones, "Wireless video coding system demonstration," Proceedings of the IEEE 1995 Data Compression Conference, pp. 448, Snowbird, Utah, March 1995.
171. Z. Gao, F. Chen, B. Belzer, and J. Villasenor, "A Comparison of the Z, E8, and Leech Lattices for image subband quantization," Proceedings of the 1995 IEEE Data Compression Conference, pp. 312-321, Snowbird, Utah, March 1995.
172. B. Schoner, J. Villasenor, S. Molloy, and R. Jain, "Techniques for FPGA Implementation of video compression," Proceedings of the ACM/SIGBA International Symposium on Field-Programmable Gate Arrays, 1995.
173. H. Chou, F. Chen, D. Valentino, L. Huang, and J. Villasenor, "Large scale implementation of optimal image compression algorithms," Proceedings of the SPIE Medical Imaging, Image Display Conference, SPIE Proceedings vol. 2431, San Diego, California ,February 1995.

174. B. Belzer, J. Liao, and J. Villasenor, "Adaptive video coding for mobile wireless networks," Proceedings of IEEE International Conference on Image Processing, pp. 972-976, Austin, Texas, 1994.
175. M.J. Tsai, J. Villasenor, and B.K.T. Ho, "Coronary angiogram video compression," Proceedings of the IEEE 1994 Nuclear Science Symposium and Medical Imaging Conference, Medical Imaging, paper No. 8M65, Norfolk, Virginia, November 1994.
176. J. Villasenor, B. Belzer, and J. Liao, "Filter evaluation and selection in wavelet image compression," 1994 IEEE Proceedings of the Data Compression Conference, pp. 351-360, Snowbird, Utah, March 1994.
177. M.J. Tsai, B.K.T. Ho, and J. Villasenor, "Motion estimation and wavelet transform in angiogram video coding," Proceedings of the 1993 IEEE Conference Record Nuclear Science Symposium and Medical Imaging Conference, vol. 2, pp.1121-1125, November 1993.
178. J. Villasenor, "Full-Frame Compression of Tomographic Images using Discrete Fourier Transform," Proceedings of the IEEE 1993 Data Compression Conference, pp. 195-203, Snowbird, Utah, April 1993.
179. H. Zebker and J. Villasenor, "Temporal decorrelation in repeat pass-radar interferometry," Proceedings of the 12th Annual International Geoscience and Remote Sensing Symposium, Houston, TX; pp. 941-943, May 1992.
180. H. Zebker, J. Villasenor, and S. Madsen, "Topographic mapping from ERS-1 and SEASAT radar interferometry," IGARSS '92; Proceedings of the 12th Annual International Geoscience and Remote Sensing Symposium, Houston, pp. 387-388, May 1992.
181. J. Villasenor and H. Zebker, "Studies of temporal change using radar interferometry," Proceedings of Synthetic Aperture Radar, Los Angeles, CA; pp. 187-198. May 1992.

Law Review and Other Academic Legal Publications

182. John Villasenor, "Ten Thousand AI Systems Typing on Keyboards: Generative AI in Patent Applications and Preemptive Prior Art," 26 *Vanderbilt Journal of Entertainment and Technology Law*, Vol. 26, p. 375, 2024.
183. John Villasenor, "Artificial Intelligence, Trade Secrets, and the Challenge of Transparency," 25 *North Carolina Journal of Law and Technology*, Vol. 25, p. 495, 2024.
184. John Villasenor, "Generative Artificial Intelligence and the Practice of Law: Impact, Opportunities, and Risks," 25 *Minnesota Journal of Law, Science, and Technology*, Vol. 25, p. 25, 2024.
185. John Villasenor, "Reconceptualizing Conception: Making Room for Artificial Intelligence Inventions," *Santa Clara High Technology Law Journal*, Vol. 39, p. 197, February 2023.
186. John Villasenor, "The First Amendment and Online Access to Information About Abortion: The Constitutional and Technological Problems with Censorship," *Northwestern Journal of Technology and Intellectual Property*, Vol. 20, p. 87, November 2022.

187. Leeza Arbatman and John Villasenor, “Anonymous Expression and ‘Unmasking’ in Civil and Criminal Proceedings,” *Minnesota Journal of Law, Science, and Technology*, Vol. 33, p. 77, January 2022.
188. Virginia Foggo and John Villasenor, “Algorithms, Housing Discrimination, and the New Disparate Impact Rule,” *Columbia Science and Technology Law Review*. Vol. 22, p. 1, January 2021.
189. Virginia Foggo, John Villasenor and Pratyush Garg, “Algorithms and Fairness,” *Ohio State Technology Law Journal*, Vol. 17, p. 123, December 2020.
190. John Villasenor and Virginia Foggo, “Artificial Intelligence, Due Process, and Criminal Sentencing,” *Michigan State Law Review*, vol. 2020, p. 295, summer 2020.
191. John Villasenor, “Views Among College Students Regarding Freedom of Expression: An Analysis in Light of Key Supreme Court Decisions,” *University of Pennsylvania Journal of Constitutional Law Online*, Vol. 20, January 2018.
192. John Villasenor, “A probabilistic framework for modelling false Title IX ‘convictions’ under the preponderance of the evidence standard,” *Law, Probability and Risk*, vol. 15, pp. 223-237, December 2016.
193. John Villasenor, “Technology and the Role of Intent in Constitutionally Protected Expression,” *Harvard Journal of Law and Public Policy*, Vol. 39, No. 3, Spring 2016.
194. John Villasenor, “Corporate Cybersecurity Realism: Managing Trade Secrets in a World Where Breaches Occur,” *American Intellectual Property Law Association Quarterly Journal*, Volume 43, Numbers 2/3, pages 329-357, Spring/Summer 2015. Available through SSRN at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2488756.
195. John Villasenor, “Rethinking a Digital First Sale Doctrine in a Post-Kirtsaeng World: The Case for Caution” *Competition Policy International Antitrust Chronicle*, Vol. 2, May 2013.
196. John Villasenor, “Observations from Above: Unmanned Aircraft Systems and Privacy,” *Harvard Journal of Law and Public Policy*, Vol. 36, No. 2, Spring, 2013.
197. Vivek Mohan and John Villasenor, “Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era” *University of Pennsylvania Journal of Constitutional Law Heightened Scrutiny*, vol. 15, October 2012.

Book

Ilana Redstone and John Villasenor, “Unassailable Ideas: How Unwritten Rules and Social Media Shape Discourse in American Higher Education,” Oxford University Press, 2020.