

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETFLIX INC. AND HULU, LLC,
Petitioners,

v.

DIVX, LLC,
Patent Owner.

Case IPR2020-00558
Patent 10,225,588

EXHIBIT 2012

DECLARATION OF SETH NIELSON, PH.D.

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. QUALIFICATIONS	2
III. APPLICABLE LEGAL STANDARDS	10
A. Priority Date of the Patent.....	10
B. Level of Ordinary Skill in the Art.....	11
C. My Understanding of Legal Standards	12
IV. PETITIONER HAS NOT DEMONSTRATED THAT A POSITA WOULD HAVE BEEN MOTIVATED TO MODIFY CHEN TO INCOPORATE PARTIAL FRAME ENCRYPTION WITH A REASONABLE LIKEILHOOD OF SUCCESS.....	14
A. Chen’s Disclosure Of Encryption Utilizes Fragment Level, Not Frame Level, Encryption.....	15
B. Chen Improves Its Latency, User Experience And Efficiency Through Features That Are Incompatible, Or Beyond The Skills Of A POSITA To Implement, With Partial Frame Encryption.	18
1. Chen’s Independent Layers And Forward Error Correction Are Integral Features That Improve The Latency, User Experience And “Efficiency” Of Its System.....	18
2. Implementing Partial Frame Encryption Together With Independent Scalable Layers And Forward Error Correction Presented Many Potentially Insurmountable Challenges Beyond The Skills Of A POSITA.	22
3. Petitioner and Dr. McDaniel Have Not Demonstrated That A POSITA Would Be Motivated To Combine Chen And Lindahl Without Chen’s Integral Features Because That Would Reduce, Not Improve, Efficiency.	28
4. The Need To Revise Standard File Formats Would Further Counsel A POSITA Against A Motivation To Combine Chen And Lindahl.....	31
V. PETITIONER DOES NOT SHOW THAT CHEN IN VIEW OF LINDAHL AND HURST RENDERS OBVIOUS “LOCATING ENCRYPTION INFORMATION...WITHIN THE REQUESTED PORTIONS OF THE SELECTED STREAM OF PROTECTED VIDEO” (ALL CLAIMS).	32

A.	The Plain Meaning Of The Claims And Every Embodiment In The '588's Specification Requires "Locating Encryption Information" "Within The Requested Portions Of The Selected Stream Of Protected Video."	33
B.	Petitioner Does Not Prove That The Lindahl/Chen Combination Teaches Or Renders Obvious Locating Encryption Information Within Requested Portions Of The Selected Stream As Claimed.	38
VI.	PETITIONER FAILS TO SHOW THAT CHEN IN VIEW OF LINDAHL AND HURST RENDERS OBVIOUS VIDEO FRAMES IN ALTERNATIVE STREAMS "THAT ARE ENCRYPTED USING A SET OF COMMON KEYS" (ALL CLAIMS).	39
A.	The Petition Fails To Show That Chen In View Of Lindahl Renders Obvious Encrypting Alternative Streams Of Video With A Common Set Of Keys.....	40
B.	The Petition Does Not Show That Chen In View Of Hurst Renders Obvious Encrypting Alternative Streams Of Video With A Common Set Of Keys.....	48
VII.	CONCLUSION.....	50

I. INTRODUCTION

I, Seth Nielson, declare as follows:

1. I have been retained on behalf of DivX, LLC (“DivX” and/or “Patent Owner”) for the above-captioned *inter partes* review to provide my expert opinions and expert knowledge. I understand that this proceeding involves U.S. Patent No. 10,225,588 (“the ’588 patent”), EX1001. I understand that the ’588 patent is currently assigned to DivX.

2. I understand that the present Petition for *inter partes* review challenges claims 1-24 (“the challenged claims” or “claims”) of the ’588 patent and was filed by Netflix Inc. and Hulu LLC (“Petitioners”) on February 15, 2020.

3. I have been asked to provide my independent review, analysis, insights, and opinions regarding technical aspects of the ’588 patent and the Petition challenging the patentability of its claims. In particular, I have been asked to provide my analysis, insights, and opinions regarding the state of the art at the time of the alleged invention and how a person of ordinary skill in the art would have understood the ’588 patent disclosure at that time.

4. In preparing this declaration, I have reviewed all of the references cited herein and in the Petition. In particular, I have reviewed and am familiar with the ’588 patent and its prosecution history, and the references cited against it, discussed further below.

5. In this declaration, I set forth the independent opinions that I have reached and the basis for those opinions in view of the information currently available to me. Such opinions are based, at least in part, on my experience for the past two decades with image and video processing, including video encryption. I reserve the right to supplement or revise my opinions should additional documents or other information be provided to me.

6. I am being compensated at an hourly rate of \$500/hour for my work on this case. My compensation is not dependent upon my opinions, my testimony, or the outcome of this case.

II. QUALIFICATIONS

7. My curriculum vitae (“CV”), a copy of which is provided as Attachment A hereto, provides details on my education, experience, publications that I have authored in the previous ten years, and a list of all cases in which, during the previous four years.

8. I received a B.S. in Computer Science in 2000 and an M.S. in Computer Science in 2004, both from Brigham Young University in Provo, Utah. I received my Ph.D. in Computer Science in 2009 from Rice University in Houston, Texas. While working towards my Ph.D. at Rice University, I studied and published research related to networking and computer security. I am the recipient of the

Brown Fellowship and a Graduate Fellowship from the Rice University Computer Science Department. I was also a John and Eileen Tietze Fellow at Rice University.

9. I am a subject matter expert in cyber security, including the sub-fields of applied cryptography and network security. I am the Founder and Chief Scientist of Crimson Vista, a boutique computer security research and consulting company. Furthermore, I am an Adjunct Assistant Professor at the University of Texas at Austin, where I teach courses on computer security in both the Computer Science department and the Law School. I am also a Distinguished Scholar and Cybersecurity Fellow at the university's Robert Strauss Center for International Security and Law.

10. In all, I have twenty years of technical experience across engineering, consulting, and academic employment, engagements, and appointments.

11. From 2001 through 2003, I worked as a software engineer at Metrowerks (formerly Lineo, Inc.), where I had substantial responsibilities relating to software architecture, computer networking, and technical project management. I also worked with our Set Top Box (STB) team investigating digital standards for transmitting video and audio data, including MPEG video streams.

12. During the 2004 fall semester of my Ph.D. program at Rice University, I identified a security vulnerability in the Google Desktop Search that could have allowed hackers to compromise users' computers and obtain private information.

After contacting Google and assisting them in closing the vulnerability, we published the details of our investigation.

13. In 2005, I completed an internship at Google, where I designed and implemented a solution to privacy loss in Google Web Accelerator. The Google Web Accelerator was designed to increase the speed of browsing the Internet. Once installed on a user's computer, the browser would request all content through a Google Proxy. The proxy performed pre-fetching and extensive caching in order to provide fast and responsive service to the user. At the time of my internship, news reports had identified odd problems in which users of the Accelerator were accessing other individual's private pages. During my internship, I designed and implemented a prototype solution for this issue in C++.

14. From 2005 through 2011, I worked as a Security Analyst and later a Senior Security Analyst for Independent Security Evaluators. There, I developed a parallel-processing based security tool, developed a FIPS-certified encryption library, developed hardware-accelerated encryption algorithms, developed encrypted file-system prototypes, developed an encryption library for an ISE client, performed port-scanning analyses, evaluated security protocols using formal methods and hand analysis, and evaluated security failures.

15. I also designed and managed the implementation of a secure communication technology that splits trust between multiple SSL Certificate

Authorities, so that if one Certificate Authority is compromised, the communication stream can still be safely authenticated. My work on the secure communications technology project led to the issuance of multiple patents. In total, I wrote hundreds of thousands of lines of code in C, C++, and Python, including projects where I had to implement the same functionality in two separate languages.

16. In 2011, I began work as a Research Scientist at Harbor Labs and continued with that consulting firm until fall 2015. I worked with a wide range of clients, specializing in network security, network communications, software architecture, and programming languages. I analyzed an extensive collection of commercial software, including software related to secure email, cloud-based multimedia delivery, document signing, anti-virus and anti-intrusion, high-performance routing, networking protocol stacks in mobile devices, PBX telecommunications software, VoIP, and peer-to-peer communications. I also analyzed security considerations for potential technology acquisitions, re-created heuristic signatures for 1995-era viruses, and re-created a 1995-era network for testing virus scanners of that time period in gateway virus scanning. I managed teams that reviewed technologies for compliance with various standards, such as HIPAA, and for security vulnerabilities.

17. Also at Harbor Labs, I reviewed technology and source code for multiple clients related to accusations of theft and/or misappropriation of trade

secrets. These engagements included an analysis of C, C++, Java, Python, and other source code languages in high-frequency trading, e-commerce, and other similar systems.

18. I also assessed the security and privacy technologies and policies provided by a third-party vendor to the Center for Copyright Infringement (CCI). CCI represents content owners, such as the RIAA and the MPAA, in finding and reducing piracy online. Because this process necessarily involves collecting information about private individuals, I was asked to investigate and determine that the information collected from online computing devices was adequately safeguarded and protected.

19. During my final year at Harbor Labs, I was engaged as the principal consultant with a large biomedical device firm in a twelve-month analysis of the security of their products. Notably, medical devices were for some time not considered significant threats in terms of computer security. However, recent demonstrations by security researchers of the various ways in which a malicious individual might harm a person using a medical device has shifted the thinking in the industry. Accordingly, I was engaged to assist this company in the analysis of their products, their process, and their future roadmap in order to ensure that patients are not harmed. I and my team analyzed design documents, hardware, and a broad range of additional resources in order to expose potential problems. The security of

these systems depends, in part, on the architecture and deployment of the networks in which they operate.

20. In March 2016, I founded Crimson Vista, Inc., a boutique technology consulting firm, with an emphasis in computer security topics. As the Chief Scientist of the company, I have consulted on computer-security topics such as the security of communications networks for financial technology (“FinTech”) companies, effective protections for website applications from intruders, and reverse engineering mobile phone security mechanisms.

21. In addition to these kinds of consulting engagements, I provide training at data conferences such as Enterprise Data World and the Data Architecture Summit. I teach data specialists how to protect data and privacy in their applications and how to be aware of data security issues in practice.

22. Through Crimson Vista, I also support the Crypto Done Right project, which aims to assist technology professionals in the correct and effective use of cryptography in their products and services. In 2019, I co-authored a book on Cryptography entitled, *Practical Cryptography in Python: Learning Correct Cryptography by Example*.

23. At Crimson Vista, I also conduct research and development projects. In 2018, I was awarded a grant from the United States Army for research into

Ransomware Mitigation. We completed our research, in conjunction with Brigham Young University, in 2019.

24. In addition to my consulting work, I maintain academic ties. In 2014, I received an appointment as a Lecturer at Johns Hopkins University and, in 2015, I advanced to an Adjunct Associate Research Scientist. From 2016 to 2019, I was also the Director of Advanced Research Projects for the Information Security Institute. During my time at Johns Hopkins University, I taught the Network Security and Advanced Network Security courses for which I created the curriculum from scratch. I published a paper about my curriculum entitled, “PLAYGROUND: Preparing Students for the Cyber Battleground.”

25. One of the components of the students’ lab work is to create a protected “sandbox” for running untrusted code. The sandbox must provide access to the system in a manner that cannot be exploited. Conversely, the other half of their assignment is to design exploitative code that attempts to bypass and/or neutralize the protections of the sandbox environment. This experimental framework enables the students to learn about creating, identifying, and neutralizing malware such as viruses.

26. In addition to my course instruction, I have also mentored Masters students at Johns Hopkins in their capstone projects. These projects include networking security and privacy concerns across a wide range of technologies

including iOS security, Bitcoin, SSL vulnerabilities, and Twitter “botnets.” These are all contemporary issues in practical computer security.

27. Although capstone projects from Masters students are not required to be publishable papers, I have had two different student teams with published results. These papers include “Potential forensic analysis of IoT data: an overview of the state-of-the-art and future possibilities” and “Cracking a Continuous Flow Reactor: A Vulnerability Assessment for Chemical Additive Manufacturing Devices.”

28. In 2018, another group of students and I produced a technical report from their capstone entitled, “Securing ADS-B Based Airborne Collision Avoidance Systems.” This project added a cryptographic protocol on top of an otherwise unsecured communications system to protect the data transfer and prevent an attacker from faking the safety messages. Our work has been submitted to an industry partner that is promoting our design and submitting it for consideration with the FAA.

29. I have since left Johns Hopkins University and have now taken an appointment as an Adjunct Assistant Professor at the University of Texas at Austin. In my new position, I teach the Network Security and Privacy class to undergraduates. My curriculum includes security topics related to cryptography and key management. I also teach the Technology of Cybersecurity in the Law School.

30. In addition to my work in consulting and academia, I have also provided expertise and guidance to government bodies. In early 2019, I testified in front of both the Maryland House of Delegates and the Maryland State Senate on matters relating to a Ransomware bill. I have also advised government antitrust agents on the key features of certain hardware security modules.

III. APPLICABLE LEGAL STANDARDS

31. When considering the '588 patent and stating my opinions, I rely on the following legal standards as described to me by the attorneys for DivX.

A. Priority Date of the Patent

32. I understand that the analysis of alleged obviousness of the Patent should be performed from the perspective of a POSITA as of the priority date of the Patent. Through a series of continuations, the Patent claims priority to September 1, 2011. The Petition asserts that the correct priority date of the Patent is December 29, 2011.

33. Because all of the references relied upon for the Petition's grounds are alleged to qualify as prior art as of the earlier priority date of September 1, 2011, I have not had the occasion, and have not been asked, to form an opinion on the priority date of the '588 Patent.

34. My opinions in this matter do not depend on whether the priority date is September 1, 2011 or December 29, 2011.

B. Level of Ordinary Skill in the Art

35. I understand that various factors should be considered when determining the person of ordinary skill in the art in connection with a particular patent. I understand that these include, without limitation: (a) the educational level of the inventors and that of practitioners and other inventors in the art (e.g., degrees, subjects, etc.); (b) the type of problems encountered in the art; (c) prior art solutions to such problems; (d) the speed at which innovations are made in the art; and (e) the sophistication of the invention.

36. Dr. McDaniel opines that a Person of Ordinary Skill In The Art (“POSITA”) would have

a bachelor’s degree in mechanical engineering, electrical engineering, computer science, or a similar field with at least two years of experience in video streaming and media security or a person with a master’s degree in mechanical engineering, electrical engineering, computer science, or a similar field with a specialization in video streaming and media security.

Ex. 1003 [McDaniel Decl.] ¶ 67.

37. As further discussed below, my opinions as stated in this declaration are valid even if the Board adopts a slightly different level of ordinary skill in the art. For example, as will be discussed throughout my report, even a person with the level of knowledge or experience described by Dr. McDaniel or adopted by the Board

would not have a reasonable expectation of success in implementing certain aspects of the proposed combination, such as implementing scalable layers with partial encryption, as of the priority date of the Patent.

C. My Understanding of Legal Standards

38. I understand that a patent claim is unpatentable if the claimed invention would have been obvious to a person of ordinary skill in the art at the time of the purported invention.

39. I understand that an obviousness analysis involves comparing a claim to the prior art to determine whether the claimed invention would have been obvious to a person of ordinary skill in the art at the time of the invention in view of the prior art and in light of the general knowledge in the art as a whole. I also understand that obviousness is ultimately a legal conclusion based on underlying facts of four general types, all of which must be considered: (1) the scope and content of the prior art; (2) the level of ordinary skill in the art; (3) the differences between the claimed invention and the prior art; and (4) any objective indicia of non-obviousness.

40. I also understand that obviousness may be established under certain circumstances by combining or modifying the teachings of the prior art. Specific teachings, suggestions, or motivations to combine any first prior art reference with a second prior art reference can be explicit or implicit, but must have existed before the date of purported invention. I understand that prior art references themselves

may be one source of a specific teaching or suggestion to combine features of the prior art, but that such suggestions or motivations to combine art may come from the knowledge that a person of ordinary skill in the art would have had.

41. I understand that a reference may be relied upon for all that it teaches, including uses beyond its primary purpose, but also including teachings that lead away from the invention. I understand that a reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, although the mere disclosure of alternative designs does not teach away.

42. I further understand that whether there is a reasonable expectation of success from combining references in a particular way is also relevant to the analysis.

43. I understand that it is improper to use hindsight to combine references or elements of references to reconstruct the invention using the claims as a guide. My analysis of the prior art is made from the perspective of a person of ordinary skill in the art at the time of the invention.

44. I am not offering any legal opinions in this declaration nor am I qualified to do so. I only consider such legal standards in framing my opinions and conclusions as well as placing assertions made by Petitioner in the Petition into the proper context. Additionally, from a subject matter perspective, I understand that the

petitioner always has the burden of persuasion regarding a challenge of patentability of an invention under an inter partes review.

IV. PETITIONER HAS NOT DEMONSTRATED THAT A POSITA WOULD HAVE BEEN MOTIVATED TO MODIFY CHEN TO INCORPORATE PARTIAL FRAME ENCRYPTION WITH A REASONABLE LIKEILHOOD OF SUCCESS.

45. I will discuss independent claim 1 in this declaration. Independent claim 12 has corresponding limitations and is not obvious for the same reasons as I discuss in connection with claim 1. All dependent claims are also not shown to be obvious at least because of their dependence from claims 1 and 12.

46. Claim 1 requires “protected video” that “includes partially encrypted frames.” Ex. 1001 [’588 Patent] cls. 1, 12. Dr. McDaniel opines that Chen “did not require any particular DRM implementation,” and thus relied upon Lindahl for the disclosure of “partially encrypted frames.” Ex. 1003 [McDaniel Decl.] ¶¶ 113, 115.

47. The Petition argues that a POSITA would have been motivated to apply Lindahl’s partial frame encryption to Chen to “address piracy concerns and improve efficiency.” Pet., 18-19. The Petition does not provide any other reason why a POSITA may be motivated to combine the references and, therefore, I address these issues here.

48. As I explain in the following paragraphs, a POSITA would not have been motivated to implement Chen’s streaming system together with Lindahl’s

partial frame encryption and also could not have made the combination with a reasonable likelihood of success.

A. Chen's Disclosure Of Encryption Utilizes Fragment Level, Not Frame Level, Encryption.

49. Dr. McDaniel opines that that Chen “did not require any particular encryption method, leaving particulars such as encryption and key management to the POSITA’s knowledge and preferences.” Ex. 1003 [McDaniel Decl.] ¶ 115. However, Chen is not silent on encryption. In the only disclosure of encryption in the reference, Chen teaches that its system performs encryption at the fragment level or block level, which is at a higher granularity than frame encryption and does not disclose partial frame encryption.

50. Chen discusses encrypting Chen’s video and highlights that “because encryption is being employed to encrypt each fragment or block separately, and thus the entire fragment or block¹ needs to be received before it can be decrypted.” Ex. 1006 [Chen] ¶ 522. A POSITA would understand this statement to mean that the entire fragment or block is encrypted as a singular unit because the entire fragment has to be downloaded before it can be decrypted. I understand that Dr. McDaniel also agrees with my understanding of this aspect of Chen. Ex. 2013 [McDaniel

¹ Chen uses fragment and block synonymously. Ex. 1006 [Chen] ¶ 74.

Depo.] 108:5-9 (“encrypting a fragment could be performed at a larger granularity than a frame”).

51. In Chen, the media content is divided into “smaller pieces, perhaps on the order of a few seconds each, to form segments.” Ex. 1006 [Chen] ¶ 63; *see also id.*, ¶¶ 153, 200-205, 293. Each segment constitutes a separate file. *Id.* (“Each segment may then be stored on a web server or CDN as a separate file.”); *see also id.*, ¶ 72 (“The terms ‘file’ and ‘segment’ are used synonymously in this document unless otherwise specified.”). At the time of the invention, each second of a movie contains roughly 25-60 frames; therefore, a segment file of, e.g., three seconds would contain about 75-180 frames. Each segment in turn consists of one or more fragments of, e.g., a half-second. *See e.g.*, Ex. 1006 [Chen] ¶ 147 (“Multiple fragments may be concatenated into a single segment ...”); ¶ 141 (“with 500 [millisecond] movie fragments”).

52. A POSITA interpreting Chen in its entirety would also recognize that there were other aspects of Chen that also confirm the understanding that Chen performs fragment level, not frame level, encryption. For example, Fig. 9(a) of Chen shows an example of Chen’s “metadata table 900,” which corresponds to the metadata provided in connection with each one of the one of plurality of “alternative streams.” Ex. 1006 [Chen] ¶ 218. As shown in Fig. 9(a), reproduced below with highlighted annotations added, DRM and encryption information are provided at a

“presentation level” (*i.e.*, for each of the alternative streams), and do not provide for any frame specific encryption information:

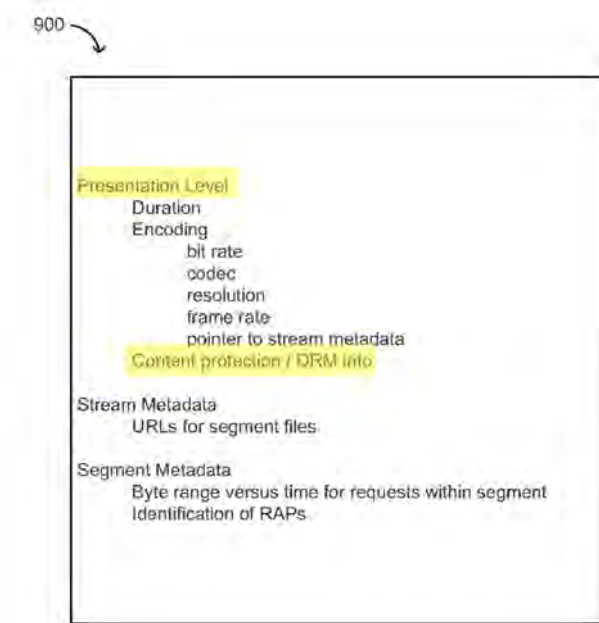


FIG. 9(a)

Ex. 1006 [Chen] Fig. 9(a); *see also id.*, ¶ 66 (“In particular, from the media presentation description, the HTTP streaming client may determine which segments in the collection can be accessed so that that the data is useful to the client capability and the user within the streaming service.”).

53. Therefore, Chen already discloses that its system utilizes fragment-level encryption, which is different from the more granular frame level encryption and does not disclose the limitation “partially encrypted frames.” As I will discuss below, a POSITA would not have been motivated to modify Chen’s encryption paradigm.

B. Chen Improves Its Latency, User Experience And Efficiency Through Features That Are Incompatible, Or Beyond The Skills Of A POSITA To Implement, With Partial Frame Encryption.

54. As I will discuss in Sections IV.B.1 and IV.B.2 below, Chen has integral features such as independent scalable layers and forward error correction, that are either incompatible with partial frame encryption or would be beyond the skills of a POSITA to implement with partial frame encryption. As I will also discuss in Sections IV.B.3, a POSITA would not have been motivated to eliminate these integral aspects of Chen just to implement partial frame encryption, because the net result would be a significant *decrease* in efficiency, and because encryption efficiency could have been achieved by methods other than partial frame encryption that were also compatible with Chen. Other factors would also have led a POSITA against Petitioner's proffered combination. *See* Section II.B.4. Therefore, a POSITA would not have been motivated to combine Chen and Lindahl as proposed by Dr. McDaniel.

1. Chen's Independent Layers And Forward Error Correction Are Integral Features That Improve The Latency, User Experience And "Efficiency" Of Its System.

55. As I will discuss below, Chen's system improves performance, user experience, and efficiency through features such as independent scalable layers and forward error correction.

56. Chen explains that one of the “novel” aspects of its system is to improve efficiency, latency, and user experience through the use of what it refers to as “independent scalability layers.” Ex. 1006 [Chen] ¶ 27 (“In some embodiments, novel improvements to methods for encoding and decoding blocks with multiple independent scalability layers are provided.”). A POSITA would understand the central importance of this feature in Chen because, among other things, Chen is titled “Enhanced Block-Request Streaming *Using Scalable Encoding*,” Ex. 1006 [Chen] Title, and all of Chen’s claims require “scalable” video encoding technique, Ex. 1006 [Chen] cls. 1, 2.

57. Through this method, the information in a given segment or fragment is divided into multiple independent, parallel layers. *Id.*, ¶¶ 375-384; Fig. 12. Each layer would represent the same section of media, but is encoded differently such that the user can start playback after it has received a subset of the layers, and the quality of playback increases as the number of layers received by the user increases. *Id*; *see also* Ex. 1006 [Chen] ¶ 381 (“[A] client that has received certain subset of the layers may perform decoding and presentation of a representation of the content.”). This improves user experience and efficiency by allowing the user to receive as many layers of the content as the network bandwidth permits, without unnecessarily stalling while waiting to receive layers that the network cannot handle due to congestion. Ex. 1006 [Chen] ¶ 379.

58. Chen's "Scalable Layers" concept is related to a process known as "Scalable Video Coding" or SVC. This basic idea behind SVC is that a high-quality stream of media is coded such that packets can be lost (either dropped or delayed until unusable) without loss in quality. Higher quality video requires more data or information in order to create the higher quality pictures. In order to stream higher quality video over a network, the network must have the capacity for the greater quantities of data. SVC is designed to permit the quality to scale based on how much data is received. Instead of simply being unable to watch the high-quality video when network conditions worsen, the SVC coding permits the quality to degrade gracefully.

59. One SVC approach mentioned by Chen, for example, is temporal scalability. Ex. 1006 [Chen] ¶ 379. Temporal coding builds extra data into the video stream that permits whole packets to be lost. This extra data is considerably smaller than the actual video data and typically includes video-specific guessing such as "motion compensation." If a packet is lost, the entire packet is "guessed" from the predictive information from the previous frames. Losing a single frame will have a negligible impact on the quality; if more packets are lost and more guesses are made, the quality degrades. Nevertheless, this may be far more acceptable than simply having the video stop altogether.

60. Another SVC approach is spatial scalability. This approach recognizes that in adaptive bitrate environments it is generally necessary to have a lower quality bitrate generated for any video. By transmitting a lower quality bitrate and higher quality bitrate together, the data for the higher quality bitrate can be reduced because much of its data can be inferred, derived, or guessed from the lower quality bitrate. This is doubly advantageous. If only the lower quality bitrate gets through, the video is still watchable in low quality. But it is also advantageous because the higher quality bitrate can be transmitted using less data. In Chen's terminology, these different bitrates are the different "layers." Chen describes an implementation with multiple layers and the more layers that are received the higher the quality of the streamed video. The more lower layers received, the better the ability to predict the higher layer, or higher quality video.

61. In addition to independent, scalable layers, another example of a technique used by Chen to improve its performance, latency, and efficiency is Forward Error Correction (FEC). FEC is a technique wherein each packet of data includes certain information about subsequent packets. Ex. 1006 [Chen] ¶ 88. Through FEC, the already received packets can supplement or correct other packets that may have parts corrupted during transmission. Chen, however, utilizes FEC as an integral part of its system to enhance efficiency by "provide[ing] protection against long and variable delivery times of data ..." Ex. 1006 [Chen] ¶ 76; *id.*, (FEC

“reduc[es] content zapping time and the variability in content zapping time.”). Chen utilizes FEC to permit its system to use already received packets to reconstruct packets that have not yet been received and start playing faster, thus improving timing performance by 70%. *Id.*, ¶¶ 529-533.

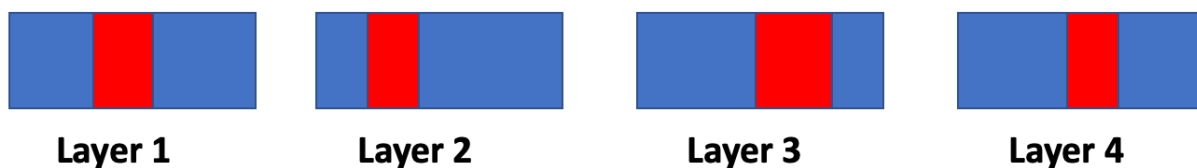
62. As I will explain in the immediately following sub-section, the above described features of Chen are either incompatible with partial frame encryption or, at the very least, are beyond the skills of a POSITA to implement with partial frame encryption.

2. Implementing Partial Frame Encryption Together With Independent Scalable Layers And Forward Error Correction Presented Many Potentially Insurmountable Challenges Beyond The Skills Of A POSITA.

63. As I will explain in this section, implementing features such as independent scalable layers and FEC together with partial frame encryption presented challenges that were beyond the skills of a POSITA.

64. As I explained in the prior section, each fragment or segment in Chen is encoded as multiple parallel, scalable layers, and a user can reconstruct the requested video using only a subset of the layers. Ex. 1006 [Chen] ¶ 381. Chen’s use of layers, however, is potentially incompatible with partial frame encryption because an unencrypted portion of one layer could be used to reconstruct the encrypted portion of a parallel layer, thus, compromising security. For example, as depicted below, an exemplary fragment in Chen has four layers, with red denoting encrypted portions

and blue denoting unencrypted portions. Information in the encrypted (red) portion of one layer may be determined from the information in the unencrypted (blue) portion of other layers:



65. For instance, if the client received both layers 2 and 4, the unencrypted portion of layer 2 could be used to fill in the encrypted portion of layer 4 and the unencrypted portion of layer 4 could be used to fill in the encrypted portion of layer 2. This would be a significant problem because it would mean that a client with no encryption key could still consume the encrypted portions of the media file. If unaddressed, this would not “address piracy,” it would aggravate security concerns.

66. Petitioner and Dr. McDaniel do not appear to explain how a POSITA could combine Lindahl’s partial frame encryption with Chen’s layers in a manner that preserves encryption and no obvious solutions are self-evident. For example, it would be impractical to attempt to encrypt identical segments of parallel layers because range of bytes in one layer does not correspond to the range of bytes in another layer and, therefore, it would be very difficult to create a system wherein only overlapping portions of layers are encrypted. *See also* Ex. 1006 [Chen] ¶ 135 (“fragments are not aligned between the different rate streams.”). But even if all

corresponding sections in different layers are encrypted, but other parts of the layers are not encrypted, it may still be possible to “infer” the encrypted data from the unencrypted portions of other layers. For example, “Temporal Scalability” (Ex. 1006 [Chen] ¶ 382), is the process of using “motion compensation” to predict where the next bits will be. When video is encoded/compressed, the smaller frames such as B and P, already use this information for compression purposes. By predicting where bits will be, not all bits have to be encoded into the encoded stream. In Temporal Scalability coding, extra information is baked into each frame to enhance this. Thus, entire frames can be lost without significant drops in quality because they can be predicted or mostly predicted. Obviously, partial encryption is useless without these components because the “predictive” information from unencrypted portion of a layer may be used to reconstruct the information in an encrypted portion of another layer.

67. Encryption with SVC is possible, however, but it would generally need to be full encryption, not partial encryption. For example, all layer data can be completely encrypted without any difficulty. The receiver decrypts all of the data and then reassembles the layers. Because all data is encrypted, there is no problem with predictive recovery. Not even every frame would have to be encrypted. In spatial scalability, the scalability is between different qualities of the same frame so encrypting all the layers of the same frame should render that frame unwatchable.

Encrypting the layers of key frames, every nth frame, or other similar such approaches would render the video unwatchable.²

68. A similar problem—unencrypted portions being used to decrypt encrypted portions—exists with attempting to implement partial frame encryption in connection with the FEC feature of Chen. As explained above, FEC provides correction information for packets in advance of the packets actually being received. If each packet is only partially encrypted, then the information from an unencrypted portion of an earlier packet may be used to decrypt the encrypted portion of a later packet without the need for the encryption key. For example, if packets 1-7 include FEC bits that allow for the reconstruction of packets 8-10, then the unencrypted portions of packets 1-7 could be used to determine the information contained in the encrypted portion of packets 8-10. This is a similar problem to the one I explained in connection with independent scalable layers.

69. Moreover, even if the issue of compromising encryption was overcome in connection with FEC, there are additional aspects of Chen's FEC that would need to be resolved if implemented with partial frame encryption. Chen utilizes FEC to reconstruct packets that have not arrived yet. In other words, earlier arrived packets will be used to reconstruct packets that have not arrived yet, without the need to

² I also note that the data cannot be encrypted prior to the SVC coding (i.e., encrypting the original, uncompressed, full quality video) because deriving the SVC layers depends on calculating interdependencies and predictive information that is lost after encryption.

actually receive those packets. Yet, Chen would not be able to actually reconstruct the not-yet-arrived packets unless it also has the encryption information, such as what portion of a frame is encrypted, in advance. Thus, unless Chen also obtains, *in advance of actually receiving the packet* that is lost in transmission, encryption parameters that identify the portions of the lost packet that are encrypted, Chen would not be able to utilize the FEC information for the lost packet. In other words, reconstructing an encrypted packet through the use of FEC data, but not being able to decrypt that reconstructed packet because the client has not yet received the encryption parameters for that packet, would render FEC useless.

70. A POSITA would not have had a reasonable expectation of success in overcoming all of the obstacles identified above. Dr. McDaniel testifies that a POSITA has only one or two years of experience in “video streaming and media security.” Ex. 1003, ¶ 67. I do not believe that a person with this level of experience could implement partial frame encryption in the context of Chen’s system. As explained above, Chen’s layers could easily compromise the encrypted portions in a partially encrypted frame because unencrypted portions of a parallel layer could be used to fill-in encrypted portions. Similarly, Chen’s use of FEC could cause a similar problem of unencrypted portions revealing encrypted portions. Even if this issue could be overcome, there are also other additional challenges such as timing and manner of transmission of encryption parameters for packets that have not yet

arrived, but are reconstructed using FEC. These are each significant hurdles that Petitioner and Dr. McDaniel do not address. I believe each of these problems is far beyond the level of skill of a POSITA because, *inter alia*, they involve complex mathematical, technical and system design aspects that well exceed the knowledge and experience of a POSITA.

71. It was also well known in the art that an encryption system was not something that was generally assembled on a system as an afterthought. Rather, it was something that needed to be designed for the underlying system. For example, as an expert in cryptography correctly explains that “[y]ou can’t make systems secure by tacking on cryptography as an afterthought,” rather, “[y]ou have to know what you are doing every step of the way, from conception through installation.” Ex. 2018 [Schneier] 1; Ex. 2017 [Schnier Blog] 1. It is also well known that there is a great difference between those that *create* cryptographic systems and those that *use* them. The entire purpose of the *Crypto Done Right* project, which I co-founded, is to better help the users of cryptography know the proper configurations and deployments of these systems. The creators of cryptography typically understand the implications of different configurations and different deployments, but this information is often not transferred well to those that use these systems. In my opinion, the POSITA described by Dr. McDaniel is, at best, a user of cryptography. If it is possible to combine partial encryption and FEC/scalable encoding, it will be

necessary to employ a person with deeper understanding of creating cryptographic systems, who would be an expert in the field, not a mere POSITA.

3. Petitioner and Dr. McDaniel Have Not Demonstrated That A POSITA Would Be Motivated To Combine Chen And Lindahl Without Chen's Integral Features Because That Would Reduce, Not Improve, Efficiency.

72. The Petition states that a POSITA would have been motivated to implement Lindahl's "partial frame encryption" in Chen to "address piracy concerns." Pet. 18. In my opinion, Petitioner and Dr. McDaniel have not shown that this is so. Chen already discloses fragment level encryption which addresses piracy concerns. There is no showing whatsoever that Lindahl's system, which only partially encrypts a frame, provides better protection or that Chen's own fragment level encryption does not provide sufficient "piracy" protection. Dr. McDaniel has provided no analysis, and I am aware of none, that Lindahl's partial frame encryption provides superior security as compared to Chen's own fragment level encryption.

73. I also disagree with Petitioner that a POSITA would have been motivated to implement Lindahl's partial frame encryption into Chen to "improve efficiency." As I explained in the immediately preceding sections, a POSITA would not have had a reasonable expectation of success in devising a partial encryption method for a system, such as Chen, that utilizes both independent scalable layers and FEC. Moreover, a POSITA would not have been motivated to eliminate those

features of Chen just to implement partial frame encryption because doing so would substantially deteriorate performance and efficiency of Chen.

74. Chen explains that, in the absence of its independent, scalable layers, user experience would be “poor” and unacceptable:

Stalls can be avoided, reduced or mitigated by restricting a data rate of the representations chosen to be much less than the available bandwidth, so that it becomes very unlikely that any given portion of the presentation would not be received in time, but this strategy has the disadvantage that the media quality is necessarily *much lower* than could in principle be supported by the available bandwidth. A lower quality presentation than is possible also can be interpreted as *a poor user experience*.

Ex. 1006 [Chen] ¶ 379.

75. Similarly, in connection with its use of FEC, Chen explains that “[t]he advantages of cooperative HTTP/TP requests together with usage of FEC repair data may be especially important to provide consistently quick channel zapping times.” *Id.*, ¶ 528. Chen then conducts an analysis of its system’s performance with and without FEC, *id.*, ¶¶ 529-533, and finds that by implementing FEC, it improved performance by up to 70%. Ex. 1006 [Chen] ¶ 533 (“Thus, in the example shown in Fig. 26, the No-FEC method is 70% worse in terms of channel zapping time than the FEC method.”); *see also id.*, Figs. 24-26.

76. Petitioner and Dr. McDaniel provide no analysis to suggest that a POSITA would have been motivated to substantially reduce performance of Chen’s system, including to cause “poor user experience” and deteriorate timing by 70%, just to implement partial frame encryption. In fact, even if a POSITA desired to reduce the encryption burden in Chen, he or she would have likely implemented the much more routine and much simpler process of encrypting some, but not all, fragments, on a periodic basis. For example, a POSITA could have encrypted, *e.g.*, every other fragment. Interestingly, the Petition argues that a POSITA “would have found it obvious to partially encrypt *all* frames,” Pet., 30, yet, it is not apparent why such partial frame encryption has any advantage to “improve efficiency” over encrypting, for example, every other fragment—especially in light of Chen’s incompatibility with partial frame encryption. Notably, encrypting some, but not all, fragments in Chen does not create the same problems identified in connection with partial frame encryption because Chen’s FEC and scalability layers are performed within individual fragments. Thus, an unencrypted fragment cannot be used to reconstruct another encrypted fragment.

77. Therefore, a POSITA would not have been motivated to combine Chen and Lindahl as proposed by Petitioner, and Dr. McDaniel has not provided any analysis to the contrary that I can respond to.

4. The Need To Revise Standard File Formats Would Further Counsel A POSITA Against Combining Chen And Lindahl.

78. Another reason a POSITA would likely not have been motivated to combine Lindahl's partial frame encryption with Chen is that this change would require a POSITA to make substantial changes to the standard file formats utilized by Chen.

79. The standard file formats contemplated by Chen such as Matroska, MP4 and 3GPP at the time of the invention did not have a structure to transfer partial frame encryption information within the file. Therefore, the combination of Chen, Lindahl and Hurst, which would require transmission of partial frame encryption in order to disclose the claims, would require a POSITA to modify the standard file formats available at the time. I understand that Dr. McDaniel agrees with the need for this modification. Ex. 2013 [McDaniel Depo.] 35:25-36:12; *see also* Ex. 2013 [McDaniel Depo.] 25:7-18; 34:11-14 (testifying that the neither the Matroska nor the MP4 and nor the 3GPP standard file formats permitted inclusion of the DRM information within the file as disclosed by the '588).

80. In my opinion, it was beyond the skills of a POSITA to modify the standard file formats to implement partial frame encryption information within the file. Notably, Petitioner's expert, Dr. McDaniel, in his declaration regarding the level of ordinary skill in the art does not opine that a POSITA would have been able to modify any of the standard file formats. Rather, Dr. McDaniel opines that the

level of ordinary skill was to merely “*us[e]* known video container file formats for streaming, such as the ISO base media file format, sometimes referred to as the MP4 container format, and 3GPP extensions to the ISO base media file format.” Ex. 1003 [McDaniel Decl.] ¶ 68.

81. This is in contrast to the disclosures of the '588 Patent, which as I will discuss in the following sections, provides a detailed disclosure on how to modify the Matroska file format to include the encryption parameters within the requested portion of the selected stream of video.

82. Therefore, this is yet another reason why a POSITA would not have been motivated to combine Chen and Lindahl and would have instead employed the traditional encryptions methods that were compatible with Chen's systems and its various features.

V. PETITIONER DOES NOT SHOW THAT CHEN IN VIEW OF LINDAHL AND HURST RENDERS OBVIOUS “LOCATING ENCRYPTION INFORMATION...WITHIN THE REQUESTED PORTIONS OF THE SELECTED STREAM OF PROTECTED VIDEO” (ALL CLAIMS).

83. Challenged independent claims 1 and 12, each require, among other things:

Locating encryption information that identifies encrypted portions of frames of video within the requested portions of the selected stream of protected video.

Ex. 1001 ['588 Patent] cls. 1, 12.

84. I understand the Board has preliminarily construed this limitation such that “within the requested portions of the selected stream of protected video” modifies “portions of frames of video.” Inst. Dec., 28-31. In other words, the recited “encryption information” can be “located” anywhere under the Board’s preliminary construction. *Id.* As I will discuss in detail in Section VI.A. below, I respectfully disagree with the Board’s provisional construction. In my opinion, a POSITA would have understood the claim language, “within the requested portions of the selected stream of protected video” modifies “locating,” and requires that the “encryption information” be “located” “within the requested portions of the selected stream of protected video.” As I will also discuss in Section VI.B. below, Lindahl, which is the sole reference relied upon by the Petition for this limitation, does not disclose this limitation, as it would have been construed by a POSITA.

A. The Plain Meaning Of The Claims And Every Embodiment In The ’588’s Specification Requires “Locating Encryption Information” “Within The Requested Portions Of The Selected Stream Of Protected Video.”

85. Both the plain meaning of the claim language to a POSITA and the ’588’s specification support that the clause “within the requested portions of the selected stream of protected video” in the “locating” step of the challenged claims modifies “locating encryption information,” and, properly construed, dictates that the “encryption information” must be “located,” “within the requested portions of the selected stream of protected video.”

86. The language of the limitation-in-question, states:

[1] ***Locating encryption information*** [2] that identifies encrypted portions of frames of video [3] ***within*** the requested portions of the selected stream of protected video

'588, cl. 1.

87. A POSITA would understand that the first clause of the limitation requires “***locating*** encryption information.” The next clause—“***that*** identifies encrypted portions of frames of video”—informs a POSITA regarding the function of the “encrypted information.” The last clause—“***within*** the requested portions of the selected stream of protected video”—informs a POSITA where the “***locat[ed]*** encrypted information” is “located.” Therefore, a POSITA would interpret the limitation as requiring the “encryption information” to be “located” “within the requested portions of the selected stream of protected video.”

88. This understanding of a POSITA from the claim language is also in accord with and is reinforced by every embodiment in the '588's specification. In ***every embodiment*** of the '588 Patent where a location for the encryption information is disclosed, “encryption information” is located within the “requested portion” of the video. Ex. 1001 ['588 Patent] 9:23-29; 13:57-63; 16:33-49; 22:14-17; 25:10-21.

89. For example, in one embodiment, the specification explains that once the requested portion of the video (referred to as a “BlockGroup”) is received, it is “parsed” for the DRMInfo (*i.e.*, “encryption information”) that identifies the

encrypted portions of the frame (*i.e.*, “locating the encryption information within the requested portions of the video”):

[E]ach of the Matroska container files containing an alternative stream of protected video includes *a DRMInfo element in a BlockGroup element containing a protected frame of video, where the DRMInfo element indicates at least a portion of the protected frames of video that is encrypted* ..., and the client application configures the processor to access video frames in a stream of protected video using the common cryptographic information by configuring the processor to: obtain a BlockGroup containing a protected frame of video; *parse the BlockGroup element to obtain a DRMInfo element indicating at least a portion of the protected frame of video that is encrypted* using an encryption key from the set of encryption keys ...

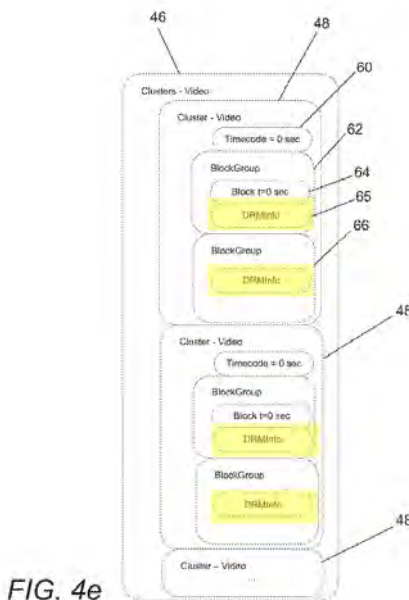
Ex. 1001 [’588 Patent] 4:39-58.

90. A POSITA would further understand that locating encryption information within the requested portions of the stream is one of the central aspects of the ’588’s inventive system. For example, the inventors did not simply utilize the industry standard Matroska container file which was not able to contain the necessary encryption information, but, rather, modified the Matroska file format to add this aspect of the invention:

In many embodiments, *the Matroska container files are specialized Matroska container files that include enhancements (i.e., elements that do not form part of the Matroska file format specification)* that

facilitate retrieval and decryption using common cryptographic information of specific portions of media during adaptive bitrate streaming.

Ex. 1001 [’588 Patent] 11:45-50. The modified Matroska container file is schematically shown in Patent’s Fig. 4e, reproduced below. As can be seen, the “DRM Info” (*i.e.*, encryption information) highlighted in yellow is located within each BlockGroup (*i.e.*, a “requested portion of the video,” ’588, 16:21-52):



Ex. 1001 [’588 Patent] Fig. 4e.

91. As noted above, I therefore respectfully disagree with the Board’s preliminary construction of this limitation. In making its preliminary claim construction, the Board quotes the ’588 at 24:63-25:2 for the proposition that the encryption information can be located anywhere and does not have to be located within the requested portions of the stream. Inst. Dec., 29-30. However, this cited

sentence relates to an index of byte ranges of the streaming media that would allow the client to select which byte ranges of the streaming media to request for viewing. This sentence does not relate to the location of **encryption information** that identifies which portions of the frames within those requested byte ranges are encrypted. As discussed above, once the selected portions of video are actually received by the client, the encryption information is located within those selected portions. Thus, the specification does not support the Board's preliminary construction.

92. The Board's preliminary construction also relied upon a grammatical treatise's guidance on best practices:

A common treatise on grammar teaches that "[t]he position of words in a sentence is the principle means for showing their relationship," and "[t]he writer must, therefore, bring together the words and groups of words that are related in thought and keep apart those that are not so related." William Strunk, Jr. & E.B. White, *The Elements of Style* 36 (4th ed. 2000).

Inst. Dec., 30. I do not believe that the grammatical preference identified by the Board would alter a POSITA's understanding of the limitation, especially in light of the '588's specification discussed above.

93. For the foregoing reasons, the "locating" limitation, as understood by a POSITA, requires that "encryption information" be "locat[ed]" "within the requested portions of the selected stream of protected video." This construction is

consistent with both the plain meaning of the claim language and every embodiment in the '588 specification.

B. Petitioner Does Not Prove That The Lindahl/Chen Combination Teaches Or Renders Obvious Locating Encryption Information Within Requested Portions Of The Selected Stream As Claimed.

94. As discussed above, the “locating” limitation of claims 1 and 12 requires “locating encryption information” “within the requested portions of the selected stream of protected video.” The Petition relies exclusively on Lindahl for the disclosure of this limitation. Pet., 52-54.

95. Petitioner relies on Lindahl’s variables X, Y, and Z teach the claimed “encryption information.” Pet., 54. But, even if Lindahl’s variables X, Y, and Z did disclose the claimed “encryption information,” Lindahl does not teach locating these variables “within the requested portions of the selected stream of protected video” as claimed.

96. Lindahl is not a streaming system in which “portions” of a “selected stream,” amongst a “plurality of alternative streams” is “requested.” Rather, Lindahl is a system in which the entire media, which is contained in a file, is downloaded for later play back. Ex. 1007 [Lindahl] ¶ 66 (“Once the media file is downloaded 708, the media file can then be decrypted 710 at the user’s local machine using the cryptographic key.”). Additionally, Lindahl only permits decryption of media once the entire media has been downloaded.

97. Therefore, the concepts of “portions” of a video and “alternative streams” simply do not exist in Lindahl. Regardless of whether Lindahl locates any encryption information, it cannot locate any encryption information within the “requested portions” of the video because a user in Lindahl can never request a portion of a video, much less one from a “selected stream.”

98. Petitioner and Dr. McDaniel do not provide any analysis for me to respond to as to why a POSITA would have sought to modify Lindahl to disclose this limitation.

VI. PETITIONER DOES NOT SHOW THAT CHEN IN VIEW OF LINDAHL AND HURST RENDERS OBVIOUS VIDEO FRAMES IN ALTERNATIVE STREAMS “THAT ARE ENCRYPTED USING A SET OF COMMON KEYS” (ALL CLAIMS).

99. Both independent claims require that video frames of the alternative streams of the protected video be “encrypted using a set of common keys comprising at least one key.” Ex. 1001 [’588 Patent] cls. 1, 12. The Petition relies on Lindahl or Hurst, in the alternative, for the disclosure of “a set of common keys,” arguing that “Lindahl and Hurst both teach or suggests *[sic]* this limitation, and either is sufficient by itself to render the limitation obvious.” Pet., 30-35. Petitioner’s arguments are incorrect for the reasons I explain below.

A. The Petition Does Not Show That Chen In View Of Lindahl Renders Obvious Encrypting Alternative Streams Of Video With A Common Set Of Keys.

100. Petitioner first relies on Lindahl for the disclosure of encrypting video frames in alternative streams of content using “a set of common keys.” Pet., 31-32. Lindahl, however, does not address the situation of encrypting video frames in multiple (alternative) streams of content, whether using the a “set of common keys” or otherwise, and thus simply cannot disclose this limitation. The concept is simply absent from Lindahl.

101. As will be discussed below, Lindahl is neither about streaming media nor does it disclose alternative streams of protected video. Lindahl utilizes a system that downloads an entire media, which is contained in a file, onto the user device, which can then access the content at a later time for playback. Ex. 1007 [Lindahl] ¶¶ 40, 66, 68. I understand that Dr. McDaniel also agrees that Lindahl does not disclose alternative streams of video. Ex. 2013 [McDaniel Depo.] 70:6-10; 71:12-16; *see also* 69:15-16 (“Lindahl does not have a direct embodiment that has streaming data in it.”).

102. That Lindahl does not disclose alternative streams of video is expected from the nature of Lindahl’s system. In Lindahl’s system, an entire media is downloaded at one time and played back later. This lies in sharp contrast to the real-time streaming challenges addressed by the ’588. The ’588 discloses that adaptive

bitrate streaming, where the user selects and switches between various alternative streams encoded at different bitrates, is a situation that arises in the context of real-time streaming media, because of fluctuations in network conditions that may affect user experience:

Adaptive bit rate streaming or adaptive streaming involves detecting the present streaming conditions (e.g., the user's network bandwidth and CPU capacity) *in real time and adjusting the quality of the streamed media accordingly* by selecting between different streams encoded for use at different network connection data rates. Typically, the source media is encoded at multiple bitrates and the playback device or client switches between streaming the different encodings depending on available resources.

Ex. 1001 ['588 Patent] 1:59-67; *see also* Ex. 1008 [Hurst] 1:31-38 (systems where “[m]edia files [are] prepared for downloading and storing usually are encoded with a higher quality audio/video than can be delivered in real time.”

103. Lindahl's disclosure uses the term “streaming” twice but neither use refers to real-time streaming of the file as described in Chen. In the first instance of use of the word “stream media,” Lindahl mentions that “[t]he remote media source 106 can transmit or stream media files to the media server 102.” Ex. 1007 [Lindahl] ¶ 39. That reference to “stream[ing]” is neither real-time nor adaptive bitrate streaming, in which media is continuously sent over the network and consumed by the user in real time, which is the kind of streaming of media that would benefit from

alternative streams. *See* Ex. 1001 [’588 Patent] 1:45-49; Ex. 1006 [Chen] ¶ 21. Instead, this reference in Lindahl to stream media is referring to the transfer of the file from the content provider to the server, not to the user. Ex. 1007 [Lindahl] ¶ 39 (“The media files that are received at the media server 102 from the media sources 104, 106 can be processed ***and then stored*** to a media storage 110.”). In that context, the word “stream” is used in the sense of transmitting files to a server for storage and later download. Transfer of files to a backend server does not even present the occasion for alternative bitrate streaming. *Id.*

104. In the second instance of the use of the word “streaming,” Lindahl mentions that “the download 708 of the media file can be performed by streaming the media file through the data network to the user, namely, to the user’s client machine.” Ex. 1007 [Lindahl] ¶ 65. This reference to “streaming” is a synonym to “transferring,” not to real-time consumption of streaming media or adaptive bitrate streaming. This is confirmed by the fact that in the immediately following step, Lindahl explains that the file cannot be decrypted until “the media file is downloaded.” *Id.*, ¶ 66.

105. Thus, Lindahl simply does not address what keys to use to encrypted “alternative streams” of protected video, whether with a set of common keys or otherwise, because the concept of alternative streams simply does not exist in Lindahl.

106. In relying on Lindahl, the Petition relies on Lindahl's disclosure relating to its use of a global key, arguing that Lindahl's global discloses the claimed "set of common keys," which a POSITA would use to encrypt "all files and videos" on the server, including alternative streams of the same video. Pet., 30-32. As I will explain below, Petitioner is incorrect because Lindahl never uses a global key to encrypt video frames, as the claims require, but only metadata.

107. First, the Petition argues that "Lindahl teaches or suggests that media files may be encrypted...with a global key." Pet., 31. This is incorrect. Lindahl never discloses that *media files* may be encrypted with a global key. Rather, Lindahl only teaches that *metadata* associated with a media file, but *not* the media data within the file, may be encrypted with a global key. Even for metadata, Lindahl teaches the use of global key only for certain metadata that "is not that sensitive" so that "stronger encryption" is not needed:

The media file is construed such that it includes media data and may further include metadata. The metadata describes characteristics of the data. For example, metadata can indicate characteristics, such as name, artist, copyright information, title, etc. The metadata of the media file is optionally encrypted, such as with a global key. In one embodiment, the *global key is used to encrypt the metadata* for all the media files at the media server. In another embodiment, if desired, different global keys can be used with different media servers. *Typically, the metadata is not that sensitive so the use of a common global key to encrypt such*

is adequate. However, if stronger encryption is desired, then more specialized keys can be used to increase the level of security.

Ex. 1007 [Lindahl] ¶ 48.

108. Lindahl's disclosure is distinct from the Patent because the claims of the Patent require encryption with a set of common keys of "video frames"—*i.e.*, video content, not merely of metadata associated with a file. *See* Ex. 1001 ['588 Patent] cl. 1, 23:43-53; Ex. 1007 [Lindahl] ¶ 48.

109. The Petition relies on a different section of Lindahl, which only states *decrypting* with a global key, to argue that Lindahl discloses encrypting all files within a server with a single global key:

Once the media file is downloaded 708, the media file can then be *decrypted* 710 at the user's local machine using the cryptographic key. The global key or other cryptographic key may also be used. If the metadata of the media file itself is encrypted, the metadata can also be decrypted using the global key which has previously been provided to the user who has purchased the access rights to the media file.

Ex. 1007 [Lindahl] ¶ 66.

110. The cited section of Lindahl quoted above does not discuss encryption, but only decryption. Therefore, it is ambiguous about the use of a global key because a POSITA would recognize that encryption and decryption both have to happen, and not necessarily with the same key. The only reference in Lindahl to encryption with a global key is at Lindahl ¶ 48, which discloses using a global key only for metadata

associated with a file, and never for actual video frames. Therefore, in the context of Lindahl, a POSITA would understand Lindahl's reference to decryption with a global key in ¶ 66 to be merely an extension of the earlier discussion in ¶ 48 where Lindahl explained the use of global key for only unimportant metadata. In fact, to interpret Lindahl to disclose using a global key for every file in a server would conflict with Lindahl's careful discussion at ¶ 48, where it explained that only unimportant metadata should be encrypted with a global key.

111. The Petition explains Lindahl's ¶ 66 by arguing that Lindahl utilizes a symmetric encryption system and therefore it is plausible to interpret the reference to "decryption" in ¶ 66 as having no corresponding reference to "encryption" in Lindahl. I disagree with this interpretation. The Petition's interpretation still does not address the conflict that would arise between Petitioner's interpretation and Lindahl's ¶ 48. Furthermore, there is no disclosure cited from Lindahl that would require Lindahl to use a symmetric key system. Lindahl's ¶ 8, which is cited by Petition at 31, discusses general background on encryption regarding the existence of both symmetric and asymmetric encryption, and does not state that Lindahl's system uses a symmetric encryption method.

112. The Petition also argues that it would be obvious to use a global key to encrypt all files within a server, and thus the alternative streams of a given video, with a global key because, Petitioner argues, Lindahl teaches that when data "is not

that sensitive...the use of a common global key to encrypt such is adequate.” Pet., 31. The Petition’s motivation has multiple flaws, as discussed below.

113. First, the Petition does not explain why, if media content were so unimportant that it would be consistent with Lindahl’s teachings to encrypt it using a single global key, the content producer or server would invest the substantial effort of encoding that “not that sensitive” content with multiple alternative bitrates to create multiple alternative streams for it to be viewed by end-users, as opposed to simply utilizing a single stream for low-priority free content. Ex. 1007 [Lindahl] ¶ 48; *compare* Pet. 31; *accord*, e.g., Hurst 19:1-6 (“Encrypt[ing] each bitrate with a different set of encryption keys ... beneficially allows for a publisher to allow a ‘standard’ user to view the movie at a lower resolution while a ‘premium’ user is allowed to watch the movie at a higher resolution or bitrate”). Lindahl itself is not a system that has multiple alternative streams itself.

114. There are many examples in the field of streaming data that are not sensitive and, therefore, are not encrypted at all. For example, when media is broadcast without the need for any restriction (e.g., geographical restriction), it is broadcast as “free-to-air,” which has no encryption whatsoever. Ex. 2020 [Free-to-view]. However, even the otherwise free broadcast does not generally use a global key but, rather, would be sent as a “free-to-view” system that would require decryption equipment. *Id.* One prominent user of such a system was BBC (British

Broadcast Corporation), which used the VideoGuard system, and which did not allow the use of a global key. *Id.*

115. A POSITA would also have little motivation to use a global key to encrypt “all files” in a given server because using a single key to encrypt an entire system would make the entire system compromised with a simple mistake by just one of the many parties involved. For example, in the 1990s, DVDs were encrypted using a global key—until the key was compromised and the entire system was rendered obsolete.³ As one observer noted, a global key system can be compromised in its entirety even where one of the many licensees who use the product inadvertently does not secure the key:

The anonymous developers of the decryption program that removes DVD copy protection had an easy time doing it, thanks to a gaffe by a software developer and the surprising weakness of the encryption technology. Essentially, the two European hackers who developed the DeCSS utility that copies a DVD movie disc were able to break the code because one of the product’s licensees inadvertently neglected to encrypt the decryption key.

Ex. 2016 [Patrizio].

³ “AACS is the successor to the Content Scramble System (CSS) [2] used to protect the content on DVDs ... Because CSS provides no mechanism for revoking a compromised key the system has been completely broken since the initial compromise.” Ex. 2019 [Henry].

116. Thus, I have not seen any analysis sufficient to motivate a POSITA to utilize a global key in the combination of Chen and Lindahl.

B. The Petition Does Not Show That Chen In View Of Hurst Renders Obvious Encrypting Alternative Streams Of Video With A Common Set Of Keys.

117. The Petition alternatively relies on Hurst for the disclosure of encrypting video frames in alternative streams of content using “a set of common keys.” Pet., 32-33. Hurst’s entire discussion of the topic is the following sentence: “The streamlets 304 of different bitrates may be encrypted with the same key.” Ex. 1008 [Hurst] 18:66-67. Significantly, Hurst’s passing reference to using the same key is immediately followed by an explanation of why it would be “beneficial” to instead “encrypt each bit rate with a different set of encryption keys”:

Alternatively, the encoder module 406 may be configured to encrypt each bit rate *with a different set of encryption keys*. *This, beneficially*, allows for a publisher to allow a “standard” user to view the movie at a lower resolution while a “premium” user is allowed to watch the movie at a higher resolution bitrate.

Ex. 1008 [Hurst] 18:64-19:6.

118. In contrast to this explicit motivation and benefit to using different keys, Hurst does not describe any benefits for using the same keys. Rather, Hurst simply acknowledges that such a configuration is possible. Even more to the point, there is no disclosure in Hurst to suggest to a POSITA that use of the same key to encrypt

alternate streams of protected video provides adequate security in a system that *also* uses partial frame encryption as disclosed by Lindahl—as using both the same key and partial encryption could negatively impact security.

119. The Petition’s proffered motivation to combine Hurst’s single, passing reference to the possibility of using the same key with Chen would not have been sufficient to bring these concepts together for a POSITA. Petitioner states:

POSITA would have been motivated to apply Hurst’s teachings—e.g., where the alternative streams are encoded at different bitrates and encrypted as a group in the same manner, such as by using the same key—because they follow the usage model for video distribution in adaptive streaming, where the playback device gains access to the alternative streams as a group. *See id.*; Ex. 1006, ¶¶[0063-0064]; §I.B. For example, a playback device adaptively streaming a movie is typically granted access to its alternative streams for the movie because it is expected to switch between them depending on channel bandwidth. Ex. 1003, ¶116. ***Since the alternative streams are accessed as a group, it would have been obvious to encrypt them as a group, using the same set of keys, so that the alternative streams can be accessed as a group using that set of keys.*** *See id.* Thus, Hurst teaches the natural and obvious approach to DRM for adaptive streaming, which a POSITA would have been motivated to apply. *Id*

Pet., 19, *citing* Ex. 1003 [McDaniel Decl.] ¶ 116.

120. There is no analysis or explanation as to why, even if multiple streams were encrypted as a group, they would be encrypted with the same key. Nor has

Petitioner provided any analysis for why encrypting with the same key would be beneficial or how any benefits may outweigh the reduced security of using a single key especially if combined with partial frame encryption, which is already inherently less secure than fully encrypted videos. For example, as discussed above, Petitioner's reference, Hurst, while disclosing the possibility of using the same key, touts the use of different keys to encrypt alternative streams of video. Ex. 1008 [Hurst] 18:64-19:6. Similarly, to the extent that Lindahl utilizes a "global key," it only teaches using it to encrypt metadata—not video frames—and even then only unimportant metadata. Ex. 1007 [Lindahl] ¶ 48. In contrast, the '558 Patent provides detailed analysis of why it utilizes a set of common keys to encrypt alternative streams of a video. Ex. 1001 ['588 Patent] 8:55-61; 10:27-31; 13:11-21; 23:46-51

121. Therefore, I do not believe Petitioner has demonstrated that a POSITA would have been motivated to combine Chen with Hurst to encrypt alternate streams of video using a set of common keys.

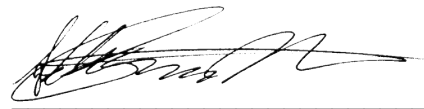
VII. CONCLUSION

122. For the foregoing reasons, Petitioner and Dr McDaniel, in my opinion, have not shown that any of the claims of the '588 Patent are obvious in view of Chen, Lindahl and Hurst.

In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required, I will appear for cross-examination within the United States during the time allotted.

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

Executed on this December 7, 2020.

A handwritten signature in black ink, appearing to read 'Seth Nielson', written over a horizontal line.

Seth Nielson, Ph.D

EXHIBIT A



Seth James Nielson's Vita

(512) 387-4310

seth@crimsonvista.com

August 2020

Academic Degrees

2010	Ph.D. Computer Science , Rice University, Houston, TX
2004	M.S. Computer Science , Brigham Young University, Provo, UT
2000	B.S. Computer Science , Brigham Young University, Provo, UT

Current Appointments

Founder and Chief Scientist	Crimson Vista, Inc.
Founder and Partner	Source Code Discovery, LLC
Adjunct Assistant Professor	University of Texas at Austin Computer Science
Cybersecurity Fellow	Robert Strauss Center for International Security and Law

Professional Advising

Cyberlab Advisory Board	The SEED School of Maryland
-------------------------	-----------------------------

Grants and Research Awards

Mitigation of Ransomware, DoD 2018.B STTR solicitation (Army), Topic: A18B-T010, Crimson Vista, \$150,000 (2019)

An Enabling Repository of Cryptographic Knowledge (Co-PI), Cisco Grant, Johns Hopkins University Information Security Institute, \$150,000 (2017-2021)

Certifications

CISSP

Subject Matter Expertise and Selected Projects

Applied Cryptography

"Crypto Done Right", Cryptographic Knowledge Base with Cisco (Johns Hopkins, 2017-2020)

Simulated implementation of Vehicle-to-Vehicle authentication (Crimson Vista, 2018-2019)

Cryptographic protocol analysis and design for Syccure Inc. (Crimson Vista, 2017-2019)

Timing attacks on Hardware Security Modules with Diamond Key Security (Johns Hopkins, 2018)

Technical consulting for U.S. Dpt. of Justice (Antitrust Division, Transportation, Energy & Agriculture) (Crimson Vista, 2018)

Aircraft/drone anti-collision protocol security with OnBoard Security (Johns Hopkins, 2017)

Cryptographic communication library for Security First Corp (ISE, 2010-2011)

Encryption library, file system encryption, GPU for Security First Corp (ISE, 2005-2011)

IoT Devices and IoT Security

Contributor, reviewer for the Institute of Assured Autonomy (Johns Hopkins, 2019)

IoT data aggregation security with Armored Things (Johns Hopkins, 2018-2019)

Automated IoT device profiling with the Physics Lab (Johns Hopkins, 2018)

Physical forensics from IoT devices (Johns Hopkins 2017)

Network Security

Information risk assessment with respect to data breach (Crimson Vista, 2020-)

Data breach analysis with respect to password authentication (Crimson Vista, 2020-)

Network security curriculum design for Law and Policy (University of Texas at Austin, 2020-)

Network security curriculum design for undergraduates (University of Texas at Austin, 2020-)

Network security curriculum design (Johns Hopkins, 2013-2019)

Security analysis of financial services vendor for Fortune-100 client (Crimson Vista, 2018-2019)

Analysis of secure e-mail transmission for confidential client (Crimson Vista, 2018-2019)

Cloud storage system security evaluation for confidential client (Harbor Labs, 2015)

Secure gateway security and compliance evaluation for SecurityFirst Corp (Harbor Labs, 2015)

Gateway caching security/privacy engineering (Google, 2005)

Malware and Viruses

Ransomware recovery research and development (Crimson Vista, 2018-2019)

Advanced malware and malware defenses analysis (Johns Hopkins, 2018)

Malware Analysis for Confidential Client (Crimson Vista, 2016)

Privacy

Development of an auditing tool for cookies and other web tracking (Crimson Vista, 2020-)

Audit of a large hospital network for cookies and web tracking (Confidential client, 2020-)

Development of a privacy curriculum for data architects (Crimson Vista, 2019)

Anonymization of threat indicators with the Applied Physics Lab (Johns Hopkins, 2017)

Analysis of anti-piracy vendor for Center for Copyright Information (Harbor Labs, 2013-2014)

Miscellaneous Security Technologies

Blockchain technology analysis for a start-up (Confidential Client, 2019-2020)

Analysis of cyber security norms for a confidential Fortune 100 client (Crimson Vista, 2018-2019)

Analysis of vulnerabilities in portable chemical manufacturing system (Johns Hopkins, 2018)

Open-Source Contribution and Sponsorship for The PyPy Project (Crimson Vista, 2018-2019)

Blockchain and smart contract design for confidential start-up (Crimson Vista, 2018)

Medical device system security evaluation for confidential client (Harbor Labs, 2015)

Software Engineering and Software Analysis

Software theft analysis and tool design for various clients (Crimson Vista, 2018-)

Cyber insurance investigations for Clyde & Co (Crimson Vista, 2018-2019)

Distributed code coverage analysis tool for a confidential Fortune 100 client (ISE, 2011)

Software engineering for Metrowerks Inc. (2001-2003, formerly Lineo Inc.)

Publications

Books

Seth James Nielson, Christopher K. Monson, Practical Cryptography in Python, Learning Correct Cryptography by Example. (October 2019).

Refereed Publications

Joseph Kosturko, Eric Schlieber, Sean Futch, Seth James Nielson, *Cracking a Continuous Flow Reactor: A Vulnerability Assessment for Chemical Additive Manufacturing Devices*. In *Proceedings of the 2018 IEEE International Symposium on Technologies for Homeland Security*. (September 2018)

Chanyang Shin, Prerit Chandok, Ran Liu, Seth James Nielson, Timothy Leschke, *Potential Forensic Analysis of IoT Data: An Overview of Amazon Echo, Z-wave, and Home Router Data Extraction and Analysis*. In *Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings)*, Exeter, UK, pp. 705-710 (June 2017).

Seth James Nielson, *PLAYGROUND: Preparing Students for the Cyber Battleground*. *Computer Science Education*, volume 26, issue 4, pp. 255-276, (January 2017).

Seth James Nielson and Charles D. Knutson, *Design Dysphasia and the Design Patterns Maintenance Cycle*. *Information & Software Technology*, volume 48, number 8, pp. 660- 675, (August 2006)

Seth James Nielson, Scott S. Crosby, and Dan S. Wallach, *A Taxonomy of Rational Attacks*. In

Proceedings of the Fourth International Workshop on Peer-to-Peer Systems (IPTPS '05), Ithaca, New York, (February 2005)

Seth J. Nielson and Charles D. Knutson. *OO++: Exploring the Multiparadigm Shift. Proceedings of the Workshop on Multiparadigm Programming with Object-Oriented Languages (MPOOL 2004)*, Oslo, Norway, (June 2004)

Rob Kunz, Seth Nielson, Mark Clement, Quinn Snell, *Effective Bandwidth for Traffic Engineering, Proceedings of the IEEE Workshop on High Performance Switching and Routing (HPSR 2001)*, Dallas, TX, (May 2001)

Testimony Before Government Bodies

Testimony in support of *Maryland SB 151/HB 211 Criminal Law - Crimes Involving Computers – Ransomware*. Testimony given to the Judicial Proceedings Committee of the Maryland Senate and the Judiciary Committee of the Maryland House of Delegates (January/February 2019)

Invited Talks, Panels, and Technical Training

Seth James Nielson, *Securing Your Data Assets Against Hackers*, 2021 Enterprise Data World, Boston, MA. (April 2021)

Seth James Nielson, *The Cybersecurity of IP*, 2020 Essential Cybersecurity Law, Austin, TX (Virtual). (July 2020)

[CANCELED DUE TO COVID 19] Seth James Nielson and Ellie Daw, *Correct Cryptography in Python*, a Tutorial for Cryptography Beginners, PyCon 2020, Philadelphia, PA. (April 2020)

[CANCELED DUE TO COVID 19] Seth James Nielson, *Protecting Your Data Assets*, 2020 Enterprise Data World, Boston, MA. (March 2020)

Seth James Nielson, *Security and Privacy for Data Architects*, 2019 Data Architecture Summit, Chicago, IL (October 2019)

Seth James Nielson, *Crypto Done Right, One Year In. Lessons Learned and Next Steps*. Presented in the International Cryptographic Knowledge Base 2019 (ICMC 2019), Vancouver, Canada (May 2019)

Panel Discussion, *Hardening US Unmanned Systems Against Enemy Counter Measures*. Accepted invitation to 7th Annual DoD Unmanned Systems Summit, Alexandria, VA (April 2019).

Seth James Nielson, *A Gentle Introduction to Blockchain*. 2019 Enterprise Data World, Boston, MA (March 2019).

Seth James Nielson, *A Gentle Introduction to Blockchain*. 2018 Data Architecture Summit, Chicago, IL (October 2018).

Seth James Nielson, *Detecting Malicious Sandboxes*. Workshop on Defensive Deception and Trust in Autonomy, San Diego, CA (August 2018).

Seth James Nielson and Debra Baker, *Towards a Crowd-Sourced Cryptographic Knowledge Base*. Presented in the International Cryptographic Knowledge Base 2018 (ICMC18), Ottawa, Canada (May 2018).

Seth James Nielson, *The PyPy Sandbox*. Presented in the National Centers of Academic Excellence Tech Talk, Online (March 2018).

Theses

PhD Thesis: Designing Incentives for Peer-to-Peer Systems (defended 10/2009)

Master's Thesis: OO++ Design Patterns, GOF Revisited (defended 8/2004)

Technical Reports

Seth James Nielson and Dan S. Wallach, The BitTorrent Anonymity Marketplace, arXiv Technical Report 1108.2718, (August 2011)

Seth James Nielson, Caleb E. Spare, and Dan S. Wallach, Building Better Incentives for Robustness in BitTorrent, arXiv Technical Report 1108.2716, (August 2011)

Seth James Nielson, Seth J. Fogarty, and Dan S. Wallach, *Attacks on Local Searching Tools*, arXiv Technical Report 1108.2704 (Originally produced in December, 2004, available on arXiv as of August 2011)

White Papers and Trade Publications

Aviel D. Rubin, Seth J. Nielson, Christopher K. Monson, *Evaluation of the MarkMonitor AntiPiracy System*, Produced for the Center for Copyright Information (December 2013)

Aviel D. Rubin, Seth J. Nielson, Sam Small, Christopher K. Monson, *Guidelines for Source Code Review in Hi-Tech Litigation*, Harbor Labs White Paper (September 2013)

Graduate Advising

Capstones for Masters of Science in Security Informatics (Johns Hopkins)

Weizhou Wang, Runjie Zhang, *Research on defense next-generation malware on the Windows platform* (December 2018)

Yu-Tsern Jou, Ying Liu, Menghan Bai, *Open Source HSM Side Channel Analysis* (December 2018)

Bowen Shi, Hong Ma, Mengqi Qin, *Side Channel Attack on HSM Based on Machine Learning* (December 2018)

Dylan Richmond, Matthew Shonman, Jingcheng Yang, *An Exploration of the Usability of HTTPS* (December 2018)

Steven Cheng, Venkata Aditya Bollapragada, and Antara Sargam, *Using Selective RAM Journaling to Fight Ransomware* (December 2018)

Yongqiang Fan, Haiwen Sun, *Fault Tolerance System for IoT* (December 2018)

Weike Chen, Harry Luo, Prashanth Venkateswaran, *IoT Discovery* (August 2018)

Joseph “Jay” Kosturko, Eric Schlieber, Sean Futch, *Cracking a Continuous Flow Reactor: A Vulnerability Assessment for Chemical Additive Manufacturing Devices* (May 2018)

Chao Lei, Wenjun Li, *Anti-Honeypot Detection in Advanced Botnet Attacks* (December 2017)

Ritvik Sachdev, Purushottam Kulkarni, Praveen Malhan, *Securing ADS-B Based Airborne Collision Avoidance Systems* (December 2017)

Ningyuan Bao, Mengying Hu, *Security-Testing-Orientated Internet of Things(IoT) Simulator* (December 2017)

Zehuan Li, Shanshan Yang, Liangjia Fu, *AIS Data De-anonymization* (December 2017)

Chanyang Shin, Prerit Chandok, Aurin Chakravarty, *Forensic Data Collection from IoT Devices* (December 2017)

Kevin Manzotti, Kashif Memon, Rahul Durgad, *Replication of CryptoDrop* (December 2016)

Harshneel More, Jingmiao Wang, Yuanqi Zhu, *Detecting XSS attacks using BRO IDS* (December 2016)

Asmaa Aljohani, Gyan Namdhari, Yue Zhu, *Feasibility, Security and Privacy Analysis of EMVCo Payment Tokenization Technology for Identity Enabled Transactions* (December 2016)

Richard Eaton, *The Emperor Has No Friends: Identifying Botnet Customers and Mapping Out Botnets on Twitter* (May 2015)

Jingru Chen, Yaning Liu, Yifan Yu, Zhiyue Zu, *Investigating the Heartbleed Vulnerability* (2015)

Kartik Thapar, *Security Techniques for Developing iOS Applications* (February 2015)

Jie Feng, Jianxiang Peng, Likai Zhang, *De-anonymizing BitCoin* (January 2014)

Teaching

University of Texas at Austin

Cybersecurity Tech/Law Policy (2020-)

Network Security and Privacy (2020-)

Johns Hopkins University

Advanced Network Security (2017 - 2019)

Network Security (2014 – Present)

Rice University

Data Structures and Algorithms (Spring 2008)

Professional Service

International Cryptographic Module Conference, 2020 Program Committee
 International Cryptographic Module Conference, 2019 Program Committee
 International Cryptographic Module Conference, 2018 Program Committee

Patents

Co-inventor: Orsini, R. 2014. Systems and methods for security data in motion. U.S. Patent 8,745,372 filed November 24, 2010 and issued June 3, 2014.

Co-inventor: Orsini, R. 2014. Systems and methods for security data in motion. U.S. Patent 8,745,379 filed August 20, 2012 and issued June 3, 2014.

Co-inventor: O'Hare, R. 2014. Systems and methods for security data. U.S. Patent 8,677,148 filed January 27, 2012 and issued March 18, 2014.

In the News

"Johns Hopkins Researchers and OnBoard Security Team Up to Protect Drones," *Robotics Tomorrow*, 3/16/2018

Academic Awards

Brown Fellowship
 John and Eileen Tietze Fellowship

Employment History

<i>University of Texas at Austin</i>	
2020-	Adjunct Assistant Professor
<i>Source Code Discovery, LLC.</i>	
2019-Present	Founder and Partner
<i>Crimson Vista, Inc.</i>	
2016-Present	Founder and Chief Scientist
<i>Johns Hopkins Applied Physics Lab</i>	
2018-2019	Senior Professional Staff (Temp/On-Call)
<i>Johns Hopkins University</i>	
2016-2019	Director of Advanced Research Projects
2015-2019	Adjunct Associate Research Scientist
2014	Lecturer
<i>Harbor Labs, LLC</i>	
2014-2015	Principal
2011-2014	Research Scientist
<i>Independent Security Evaluators</i>	
2010-2011	Senior Security Analyst

2005-2009 **Security Analyst**

Google, Inc.
2005

Summer Intern

Metrowerks (Formerly Lineo, Inc.)
2001-2003

Software Engineer II

Expert Testimony

On behalf of Magic Micro in Monsoon v. Magic Micro (2020-Present)

Counsel: Gutnicki, LLP
Venue: International Centre for Dispute Resolution
Subject Matter: Blockchain, file storage
Reports: 1 declaration submitted October 2020
1 declaration submitted November 2020

On behalf of Juniper in Juniper Networks Inc. v. Huawei Digital Technologies Co. (2020-Present)

Counsel: Irell and Manella, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Network perimeter defense against malware
Reports: 1 declaration submitted June 2020

On behalf of DivX in Netflix v. DivX (2020-Present)

Counsel: Lowenstein & Weatherwax, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Encryption of streaming media
Reports: 1 declaration submitted May 2020

On behalf of Juniper in Juniper Networks Inc. v. Implicit LLC (2019-2020)

Counsel: Irell and Manella, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Packet classification
Reports: 1 declaration submitted February 2020

On behalf of the Dealership class in Dealer Management Systems Antitrust Litigation (2019-Present)

Counsel: Milberg Phillips Grossman LLP
Venue: Case No. 18-cv-00864 (Northern District of Illinois)
Subject Matter: Cybersecurity, risk assessment, third-party access
Reports: 1 report submitted November 2019
Deposition: January 2020

On behalf of Symantec in the Trustees of Columbia University in the City of New York v. Symantec Corporation. (2018-Present)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Case No. Civil Action No. 3:13-cv-00808-JRS (Eastern District of Virginia)
Subject Matter: Deception technologies, Honeypots
Reports: 1 report submitted October 2019

Deposition: January 2020

On behalf of Proofpoint in Proofpoint Inc. v. Vade Secure (2019-Present)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
 Venue: Case No. 3:19-cv-04238 (Northern District of California)
 Subject Matter: Cloud-based email, malware detection, AI
 Reports: 1 report submitted September 2019, 1 report submitted December 2019

On behalf of Bitdefender in Finjan Inc. v. BitDefender Inc. (2018-Present)

Counsel: Susman Godfrey LLP
 Venue: Case No. 4:17-cv-4790-HSG (Northern District of California)
 Subject Matter: Web threat detection, malware, gateways
 Reports: 1 report submitted July 2019, 1 report submitted August 2019
 Depositions: October 2019

On behalf of HTC in Koninklijke Philips N.V., US Philips Corporation v. HTC Corp., HTC America Inc. (2019-Present)

Counsel: Perkins Coie LLP
 Venue: Case No. 4:18-cv-01887-HSG (Northern District of California)
 Subject Matter: Cryptographic protocols
 Reports: 1 report submitted May 2019, 1 report submitted June 2019
 Depositions: August 2019

On behalf of Juniper in Juniper Networks Inc. v. Finjan Inc. (2018-Present)

Counsel: Irell and Manella, LLP
 Venue: PTAB Petition for Inter Partes Review
 Subject Matter: Malware, firewall/gateway, network security
 Reports: 4 declarations submitted October 2018
 Depositions: June 2019

On behalf of Redbox in Disney Enterprises, Inc., LucasFilm Ltd, LLC, and MVL Film Finance LLC v. Redbox Automated Retail, LLC. (2018)

Counsel: Robins Kaplan LLP
 Venue: Case No. 2:17-cv-08655-DDP (AGRx) (Central District of California, Western Division)
 Subject Matter: DRM, cloud security, media streaming
 Reports: 1 declaration submitted May 2018

On behalf of Trend Micro in Trend Micro, Inc. v. Security Profiling, LLC (2017-2018)

Counsel: The Marbury Law Group, PLLC
 Venue: Inter Partes Review Case No. IPR2017-02191 and IPR2017-02192
 Subject Matter: Automated security patches
 Reports: 2 declarations submitted September 2017
 Depositions: June 2018

On behalf of TeleSign in Twilio Inc. v. TeleSign Corporation (2016-Present, multiple cases)

Counsel: Shook, Hardy & Bacon LLP
 Venue: Inter Partes Review Case No. IPR2016-01688, IPR2016-00360, IPR2017-01976 IPR2017-01977, IPR2017-01978

Case No. 5:16-cv-6925-LHK (Nor. District of California, San Jose Div.)
 Subject Matter: Telecommunications security
 Reports: 1 declaration submitted August 2016, May 2017, and July 2017
 Depositions: November 2016, July 2017, August 2017

On behalf of Blue Coat in Finjan Inc. v. Blue Coat Systems LLC (2017-2018)

Counsel: Originally Wilson, Sonsini, Goodrich and Rosati PC; later Morrison & Foerster LLP
 Venue: Case No. 15-cv-03295-BLF-SVK (Nor. District of California, San Div.)
 Subject Matter: Firewalls, gateway, security devices, malware
 Reports: 1 report submitted April 2017
 Depositions: April 2017
 In Court: Tech tutorial February 2017, expert testimony November 2017

On behalf of Sedosoft in Sedosoft Inc. v Mark Burchett LTD and NFSx9 LLC (2016)

Counsel: McInnes and McLane LLP
 Venue: Case No. Civil Action No. 1:15-cv-10244-RGS (District of Massachusetts)
 Subject Matter: Code theft
 Reports: 1 report submitted May 2016 and August 2016

On behalf of USAA in Asghari-Kamrani, et al. v. United Services Automobile Association, Inc.

Counsel: Fish and Richardson PC
 Venue: Inter Partes Review Case No. IPR2015-01842, and CBM2016-00063, CBM2016-00064
 Subject Matter: Applied cryptography, authentication
 Reports: 1 report submitted September 2015, 1 report submitted April 2016
 Depositions: March 2017

On behalf of WTS Paradigm in WTS PARADIGM, LLC v EDGEAQ, LLC (2015-2016)

Counsel: Quarles & Brady LLP
 Venue: Case No. 3:15-CV-330 (Western District of Wisconsin)
 Subject Matter: Software-assisted product configuration, presentation, and ordering
 Reports: 1 report submitted March 2016
 Depositions: April 2016

On behalf of Mr Leon Stambler in Mr. Leon Stambler v Mastercard IPR (2015-2016)

Counsel: Flachsbarth & Greenspoon, LLC
 Venue: CBM2015-00044
 Subject Matter: Authentication, authentication codes
 Reports: 1 declaration submitted October 2015
 Deposition: December 2015

On behalf of Trusteer/IBM in Trusted Knight Corporation v. International Business Machines Corporation and Trusteer, Inc. (2015)

Counsel: Quinn Emanuel Urquhart & Sullivan LLP
 Venue: C.A. No. 14-1063 LPS-CJB (District of Delaware)
 Subject Matter: Key logging, protections against
 Reports: 1 declaration submitted July 2015

On behalf of Sensus in Sensus USA, Inc. v. Certified Measurement, LLC (2015)

Counsel: Feldman Gale PA
 Venue: Inter Partes Review Case No. IPR2015-01262, IPR2015-01311, IPR2015-01439, IPR2015-01454
 Case number 3:14-cv-01069 (District of Connecticut)
 Subject Matter: Applied cryptography, certification of data
 Reports: 1 declaration submitted June 2015, 4 declarations submitted July 2015

On behalf of Chad Eichenberger in Chad Eichenberger v. ESPN (2015)

Counsel: Edelson PC
 Venue: Case No. 2:14-cv-00463 (Western District of Washington)
 Subject Matter: Consumer privacy
 Reports: 1 declaration submitted January 2015

On behalf of Optimum Content Protection in Microsoft Corporation v. Optimum Content Protection LLC. (2014)

Counsel: Sidley Austin LLP
 Venue: Inter Partes Review No. IPR2015-00048
 Subject Matter: DRM, data streaming, protection
 Reports: 1 declaration submitted October 2014

On behalf of Fortinet in Fortinet v. Sophos (2014-2015, multiple cases)

Counsel: Quinn Emanuel Urquhart & Sullivan LLP
 Venue: Inter Partes Review No. IPR2015-00618
 Case No. 3:13-cv-05831-EMC (DMR) (Nor. District of California, SF div.)
 Case No. 1:14-cv-00100-GMS (District of Delaware)
 Subject Matter: Antivirus, anti-malware
 Reports: 2 declarations submitted September 2014, 1 submitted September 2015
 1 report submitted October 2015, November 2015
 Depositions: October 2014, October 2015
 In Court: Tech tutorial December 2015

On behalf of Afiliis in Afiliis PLC v Architelos Inc and Alexa Raad (2015)

Counsel: Haynes Boone LLP
 Venue: Case No. 1:15-cv-00014-LMB-JFA (Eastern District of Virginia)
 Subject Matter: Domain name system anti-abuse
 Reports: 1 report submitted April 2015, May 2015
 Depositions: June 2015
 In Court: Expert testimony August 2015

On behalf of Telit in M2M v. Motorola, Telit (2015-2016)

Counsel: Pearl Cohen Zedek Latzer Baratz LLP
 Venue: Case No. 12-033-RGA (District of Delaware)
 Subject Matter: Authentication
 Reports: 1 declaration submitted May 2014,
 1 report submitted July 2014, August 2014
 Depositions: June 2015

On behalf of Rmail/Rpost in Rmail Limited, v. Amazon.com, Inc., and Paypal and Rmail Limited,

Rpost Communications Limited, and Rpost Holdings Inc., v.Docusign, Inc. (2013-2014)

Counsel: Hudnell Law Group PC
Venue: Case No. 2:10-CV-258-JRG (Lead Case)
Case No. 2:11-CV-299-JRG (Member Case) (E.D. Texas)
Subject Matter: Email security
Reports: 2 reports April 2013, 1 declaration June 2013
Depositions: May 2013 (2 days)

On behalf of Via Vadis in Via Vadis v. Skype (2012-2014)

Counsel: WTP Law
Venue: Via Vadis v. Skype, Case No. 11-507 (RGA) (District of Delaware)
Subject Matter: P2P communications
Reports: 1 affidavit December 2012