

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURITY FIRST INNOVATIONS, LLC,
Patent Owner.

Case No. IPR2024-00212
Patent No. 11,178,116

EXHIBIT 2033

**SECOND DECLARATION OF AVIEL D. RUBIN, PH.D.
IN SUPPORT OF PATENT OWNER'S RESPONSE**

TABLE OF CONTENTS

I. INTRODUCTION 1

II. QUALIFICATIONS.....1

III. BASES OF OPINIONS 7

IV. APPLICABLE LEGAL STANDARDS 10

A. Level Of Ordinary Skill In The Art.....10

B. My Understanding Of Legal Standards.....12

V. CLAIMS-AT-ISSUE (CLAIMS 1-14) 15

VI. OPINIONS.....16

A. Overview Of The '116 And The Challenged Claims 16

B. Petitioner’s Tajima Ground Fails (All Claims, Grounds 1-4). 17

 1. Tajima Does Not Disclose “Separately Storing Each Data
 Chunk ... Together With One Of The Plurality Of Obfuscated
 Different Encryption Keys” (Limitation 1[d])..... 17

**C. Petitioner’s Tajima/Foster, Tajima/Rivest, and Tajima/Rivest-
 Shyu Grounds Fail (Grounds 2, 3, and 4; Claims 1-3, 6, 9-14).....22**

 1. The Tajima-Foster Ground Fails (Ground 1; Claims 1-2, 9, 11-
 14). 23

 2. A POSITA Would Not Be Motivated to Combine Tajima &
 Rivest (Ground 3, Claims 9-14)..... 38

 3. A POSITA Would Not Have Motivation to Combined Tajima,
 Rivest, and Shyu (Ground 4; Claims 1-3, 6)..... 41

- 4. Petitioner’s Explanation of Proposed Motivations to Combine Tajima/Foster, Tajima/Rivest and And Tajima/Rivest/Shyu Do Not Consider Drawbacks And Are Purely Hindsight Driven.. 45

D. The Foster-Hayhurst Ground Fails (Ground 5; Claims 1-2, 5, 9, and 11). 47

- 1. Hayhurst is Not Analogous Art to the ’116 Patent. 47
- 2. The Petition Fails to Establish Any Motivation to Combine Foster and Hayhurst. 53

VII. CONCLUSION 74

I. INTRODUCTION

1. My name is Aviel D. Rubin. I have been retained as an expert witness to provide my independent opinion in regard to the matters at issue in *inter partes* review of U.S. Patent No. 11,178,116 (“the ’116 patent”) in IPR2024-00212. I have been retained by Security First Innovations, LLC (“SFI”), the Patent Owner in this proceeding. Petitioner is Google LLC (“Google” or “Petitioner”).

2. I am being compensated \$925 per hour for my time spent working in connection with this case. My compensation is in no way related to the outcome of this litigation. If called as a witness, I would testify as to the statements and opinions contained in this report.

3. I am not a legal expert and offer no opinions on the law. However, I have been informed by counsel of the various legal standards that apply, and I have applied those standards in arriving at my conclusions.

II. QUALIFICATIONS

4. I have more than 30 years of experience in the fields of computer science and applied cryptography. My professional career has been dedicated to issues relating to software, networks, and computer systems more generally, including issues relating to computer and information security.

5. I received a Bachelor of Science in Computer Science with Honors from the University of Michigan in 1989, a Master of Science in Computer Science and Engineering from the University of Michigan in 1991, and a Ph.D. in Computer Science and Engineering from the University of Michigan in 1994. My Ph.D. dissertation was titled “Nonmonotonic Cryptographic Protocols” and concerned authentication in long-running network operations.

6. I am a Professor Emeritus in Computer Science at Johns Hopkins University (the “University”). I joined the Computer Science faculty at the University in 2003 and was promoted to full professor with tenure in April 2004. As a member of the faculty, I perform research, teach graduate and undergraduate courses in computer science and related subjects, advise undergraduate and Masters students, and supervise the research of Ph.D. candidates and other students. I have taught courses including Networking, Security and Privacy in Computing, Cryptography, and Advanced Topics in Computer Security, among others. In September 2023, I was appointed Professor Emeritus.

7. I also served as the Technical Director of the University’s Information Security Institute (“ISI”). The ISI is the University’s focal point for research and education in information security, assurance, and privacy. The University, through the ISI’s leadership, has been designated as a Center of Academic Excellence in

Information Assurance by the National Security Agency and leading experts in the field.

8. I also have significant industry experience. Since 2011, I have served as the founder and chief scientist of Harbor Labs, a software and networking consulting firm specializing in data security and privacy. Previously, from 2005 to 2011, I served as the founder and President of Independent Security Evaluators (“ISE”), a computer security consulting firm. In that capacity, I guided ISE through the qualification process to become an independent testing laboratory for Consumer Union, which produces the Consumer Reports magazine. ISE provided consulting services to various companies on potential security flaws and weaknesses in products and systems. These companies included Fortify Software, Verdasys, and Security First Corp. As an independent testing laboratory for Consumer Union, I managed an annual project where we tested popular anti-virus products. Our results were published in Consumer Reports each year for three consecutive years.

9. In addition, I came to the University from AT&T Labs, Secure Systems Research Department, where I spent six years focused on Internet and computer security. Prior to AT&T Labs, I spent two years at Bellcore in its Cryptography and Network Security Research group, also focusing on Internet and computer security

issues. I also interned at IBM in 1989. During my time there, I worked on the IBM System/360 family of mainframe computer systems.

10. I am the author or co-author of five books regarding information security issues: *Brave New Ballot*, Random House, 2006; *Firewalls and Internet Security* (second edition), Addison Wesley, 2003; *White-Hat Security Arsenal*, Addison Wesley, 2001; *Peer-to-Peer*, O'Reilly, 2001; and *Web Security Sourcebook*, John Wiley & Sons, 1997.

11. I have received numerous awards for my work and research in the field of computer security, including:

- In 2020, I received the Distinguished Service Award from the Institute of Electrical and Electronics Engineers (“IEEE”) Computer Society Technical Committee on Security and Privacy;
- In 2010, I received a Fulbright Scholarship to serve as a Visiting Professor at Tel Aviv University in Israel;
- In 2009, I received a Google Research Award for my work on securing medical records on smartphones;
- In 2007, I received the Privacy Enhancing Technologies Award for Outstanding Research for my work on a security analysis of a cryptographically enabled RFID device;

- In 2004, I was named Baltimorean of the Year by Baltimore Magazine for my work in safeguarding the election process;
- In 2004, I received the Electronic Frontiers Foundation Pioneer Award; and
- In 2000, I received the Best Paper Award at the 9th USENIX Security Symposium.

12. I serve, or have served, on several technical and editorial advisory boards. For example, I served on the Editorial and Advisory Board for the International Journal of Information and Computer Security. I also served on the Editorial Board for the Journal of Privacy Technology. In addition, I have been Associate Editor of the IEEE Security and Privacy Magazine and served as Associate Editor of the Association for Computing Machinery's ("ACM") Transactions on Internet Technology. I also served as Associate Editor of the journal Communications of the ACM, and I was an Advisory Board Member of Springer's Information Security and Cryptography Book Series. I also have served in the past as a member of the Defense Advanced Research Projects Agency's Information Science and Technology Study Group, a member of the Government Infosec Science and Technology Study Group of Malicious Code, a member of the AT&T Intellectual Property Review Team, Associate Editor of the Electronic Commerce

Research Journal, Co-editor of the Electronic Newsletter of the IEEE Technical Committee on Security and Privacy, a member of the board of directors of the USENIX Association (the leading academic computing systems society), and a member of the editorial board of the Bellcore Security Update Newsletter.

13. I have spoken on information security and electronic privacy issues at more than 50 seminars and symposia. For example, I presented keynote addresses on the topics “Security of Electronic Voting” to Computer Security 2004 Mexico in Mexico City, Mexico, in May 2004; “Electronic Voting” to the Secure Trusted Systems Consortium 5th Annual Symposium in Washington, D.C., in December 2003; “Security Problems on the Web” to the AT&T EUA Customer Conference in March 2000; and “Security on the Internet” to the AT&T Security Workshop in June 1997. I also presented a talk about hacking devices at the TEDx conference in October 2011 and another TEDx talk on the same topic in September 2015.

14. I am a named inventor on 10 United States patents, including U.S. Patent Nos. 5,638,446 (“Method for the Secure Distribution of Electronic Files in a Distributed Environment”) and 5,809,140 (“Session Key Distribution Using Smart Cards”).

15. A detailed record of my professional qualifications is set forth in the attached Exhibit A, which is my *curriculum vitae*, including a list of publications,

awards, research grants, and professional activities. My *curriculum vitae* also lists the matters in which I have served as an expert.

III. BASES OF OPINIONS

16. In the course of conducting my analysis and forming my opinions, in addition to the Petition in this proceeding I have reviewed materials including those listed below:

- i. U.S. Patent No. 11,178,116 (EX1001) (“the ’116 patent” or “’116”);
- ii. The prosecution history of the ’116 Patent (EX1002)
- iii. The Declaration signed by Samrat Bhattacharjee, Ph.D. in IPR2024-00212 (EX1003) (the “Bhattacharjee Declaration”);
- iv. The Curriculum Vitae of Samrat Bhattacharjee, Ph.D. (EX1004)
- v. The Petition by Google in IPR2024-00212;
- vi. U.S. Patent Application Publication 2003/0028493 (“Tajima”) (EX1005);
- vii. U.S. Patent Application Publication 2003/0200176A1 (“Foster”) (EX1006);
- viii. International Application Publication WO 2004/008289A2 (“Hayhurst”) (EX1007);

- ix. U.S. Provisional Application 60/396357 (“Hayhurst-Provisional”) (EX1008);
- x. Coversheet of U.S. Provisional Application 60/396357 (EX1009);
- xi. Application Data for Provisional Application 60/396357 (EX1010);
- xii. Security First Innovation’s 2023-08-14 Infringement Contentions, Chart A (EX1011);
- xiii. Security First Innovation’s 2023-08-14 Infringement Contentions, Chart C (EX1012);
- xiv. U.S. Patent Application Publication 2004/0049687 (EX1013);
- xv. International Application Publication WO 2001/22322 (EX1014);
- xvi. U.S. Patent No. 10,452,854 (EX1015);
- xvii. U.S. Patent No. 6,021,391 (EX1016);
- xviii. U.S. Patent Application Publication 2004/0049700 (EX1017);
- xix. U.S. Patent Application Publication 2004/0003272A1 (EX1018);
- xx. International Application Publication WO 2001/015162A2 (EX1019);
- xxi. U.S. Patent Application Publication 2002/0194209 (EX1020);
- xxii. U.S. Patent No. 6,819,766 (EX1021);
- xxiii. U.S. Patent No. 4,238,853 (EX1022);
- xxiv. U.S. Patent No. 7,277,941 (EX1023);

- xxv. U.S. Patent Application Publication 2005/0216754 (EX1024);
- xxvi. International Application Publication WO 2004/057461A2 (EX1025);
- xxvii. U.S. Patent No. 7,178,033 (EX1026);
- xxviii. U.S. Patent No. 6,490,353 (EX1027);
- xxix. U.S. Patent Application Publication No. 2003/0167314 (EX1028);
- xxx. U.S. Patent No. 7,529,834 (EX1029);
- xxxi. U.S. Patent Application Publication 2001/0037474A1 (EX1030);
- xxxii. U.S. Patent Application Publication 2004/0172476A1 (EX1031);
- xxxiii. U.S. Patent No. 7,099,994 (EX1032);
- xxxiv. U.S. Patent No. 6,151,659 (EX1033);
- xxxv. R. L. Rivest, “*All-or-nothing encryption and the package transform*,”
Proc. Of the 4th Intl. Workshop on Fast Software Encryption 1997, (E.
Biham, ed.), Lecture Notes in Computer Science, 1267 (1997) pp. 210-
218. (“Rivest”) (EX1034);
- xxxvi. U.S. Patent No. 6,308,277 (EX1035);
- xxxvii. U.S. Patent Application Publication 2001/0053221A1 (EX1036);
- xxxviii. Security First Innovation’s 2023-08-14 Infringement
Contentions, Chart D (EX1037);
- xxxix. U.S. Patent Application Publication 2018/0367509A1 (EX1039);

- xl. ABS: The Apportioned Backup System (EX1040);
- xli. U.S. Patent Application Publication 2003/0081790A1 (EX1041);
- xlii. Google LLC's Proposed Claim Terms for Construction (EX1042);
- xliii. Letter from A. Mayron to D. Perlson re Preliminary Proposed Constructions (EX1043);
- xliv. U.S. Patent No. 9,338,140 (EX1044);
- xlv. The Institution Decision in IPR2024-00212.
- xlvi. The exhibits and other documents cited herein.

IV. APPLICABLE LEGAL STANDARDS

A. Level Of Ordinary Skill In The Art

17. My opinions in this declaration are based on the understanding of a person of ordinary skill in the art, which I understand is sometimes referred to as an “ordinary artisan” or by the acronyms “POSA,” “POSITA” or “PHOSITA,” as of the time of the invention, which I understand is here assumed to be the effective filing date (October 25, 2004) of the provisional application from which the ’116 patent issued. I understand that the person of ordinary skill in the art is a hypothetical person who is presumed to have known the relevant art at the time of the invention. By “relevant,” I mean relevant to the challenged claims of the ’116 patent.

18. I understand that factual indicators of the level of ordinary skill in the art include the various prior art approaches employed, the types of problems encountered in the art, the rapidity with which innovations are made, the sophistication of the technology involved, and the educational background of those actively working in the field. I understand that, in assessing the level of skill of a person of ordinary skill in the art, one should consider the type of problems encountered in the art, the prior solutions to those problems found in the prior art references, the rapidity with which innovations are made, the sophistication of the technology, the level of education of active workers in the field, and my own experience working with those of skill in the art at the time of the invention.

19. In this case, Dr. Bhattacharjee has asserted in his declaration that a person of ordinary skill in the art as of the time of the '116 patent would have had:

at least a bachelor's degree in computer science, computer engineering, or a related field, with three (3) years of experience in the area of securing data from unauthorized access or use. *See, e.g.*, EX1001, 1:21-

22. A higher level of education may substitute for less experience.

EX1003¶ 44.

20. For the purposes of this declaration, I accept Dr. Bhattacharjee's proposed qualifications of a POSITA.

21. As will be discussed throughout my report, even a person with the level of knowledge or experience described by Dr. Bhattacharjee would not have a motivation or reasonable expectation of success in implementing certain aspects of the proposed combination as of the priority date of the '116 patent.

B. My Understanding Of Legal Standards

22. When considering the '116 patent and stating my opinions, I rely on the following legal standards as described to me by the attorneys for SFI.

23. I understand that a patent claim is unpatentable if the claimed invention was anticipated by a prior art reference or would have been obvious to a person of ordinary skill in the art at the time of the purported invention.

24. I understand that anticipation requires that every limitation of the claim at issue be disclosed, either expressly or under principles of inherency, in a single prior art reference.

25. I understand that inherency may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient. Instead, it must be proven that the claim limitation not expressly found in the reference necessarily follows from what is found there.

26. 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 (“POSITA”) 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, including any praise of the invention.

27. 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.

28. It is my understanding that a reference qualifies as prior art for an obviousness determination only when it is analogous to the claimed invention. To be analogous, I understand that a reference must be either (1) from the same field of

endeavor as the patent-at-issue, or (2) reasonably pertinent to the particular problem with which the inventor of the challenged patent is involved.

29. 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 POSITA may not be motivated to combine or modify references when a person of ordinary skill, upon reading the references, would be discouraged from following the path they set out.

30. It is my understanding that the purposes of both the invention and the prior art are important in determining whether the reference is reasonably pertinent to the problem the invention attempts to solve. It is also my understanding that when addressing whether a reference is analogous art with respect to a claimed invention under a reasonable-pertinence theory, the problems to which both relate must be identified and compared. Thus, if the reference is directed to a different purpose, it is my understanding that the inventor would accordingly have had less motivation or occasion to consider it.

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

32. 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 POSITA at the time of the invention.

33. 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.

V. CLAIMS-AT-ISSUE (CLAIMS 1-14)

34. I understand that Petitioner has challenged the claims as follows:

- Independent claim 1 and its dependent claims 5-8 based on anticipation and/or obviousness over Tajima (Ground 1);
- Independent claim 1, its dependent claim 2, independent claim 9, and its dependent claims 11-14 based on obviousness over Tajima and Foster (Ground 2);
- Independent claim 9 and its dependent claims 10-14 based on obviousness over Tajima and Rivest (Ground 3);
- Independent claim 1 and its dependent claims 2-3 and 6 based on obviousness over Tajima, Rivest, and Shyu; and

- Independent claim 1, its dependent claims 2 and 5, independent claim 9, and its dependent claim 11 based on obviousness over Foster and Hayhurst.

VI. OPINIONS

A. Overview Of The '116 And The Challenged Claims

35. The '116's claimed inventions, and related disclosure, concern securing data within a system. EX1001 ['116] 1:28-33 (“computer systems ... are often storing, archiving, and transmitting all types of sensitive information. Thus, an ever-increasing need exists for ensuring data stored and transmitted over these systems cannot be read or otherwise compromised.”). The '116 further teaches that it is undesirable for stored data to “remain[] whole and intact and subject to attack.” *Id.*, 57:12-13. To address this need, the '116 teaches methods in which a dataset is processed with a “cryptographic parsing and splitting ... into two or more portions or shares,” secured with “another layer of encryption to each share of the data,” and then stored such that shares are in “different physical and/or logical locations.” *Id.*, 57:14-24.

36. The claims of the '116 require parsing the dataset into chunks, encrypting those chunks with distinct encryption keys, obfuscating or transforming those encryption keys, and then storing the data chunks on a plurality of different

storage devices. *Id.*, cls. 1, 9. Each of these steps is intended to secure the dataset. “[C]ryptographic parsing and splitting” of the dataset into chunks and “physical[] remov[al]” of the encrypted and “further secure[d]” chunks from the system onto a plurality of different storage devices removes the possibility of “attack” or “compromise” of the whole dataset. *Id.*, 57:13-24.

B. Petitioner’s Tajima Ground Fails (All Claims, Grounds 1-4).

1. Tajima Does Not Disclose “Separately Storing Each Data Chunk ... Together With One Of The Plurality Of Obfuscated Different Encryption Keys” (Limitation 1[d]).

37. Independent claim 1 requires:

Limitation 1[d] “separately storing each data chunk of the plurality of data chunks together with one of the plurality of obfuscated different encryption keys on a plurality of different storage devices.”

38. I understand that in each of its Tajima-based grounds, Petitioner argues that Tajima discloses (as would be required for anticipation) and/or renders obvious this limitation by teaching attaching “information regarding the key” (also called “key information” in Tajima) to the data fragments. Pet., 20-22, 24 (“Tajima separately stores each encrypted data fragment together with an ‘*obfuscated different encryption key*’ (i.e., the key information that encrypted the other data fragment) on ‘*a plurality of different storage devices*’ (i.e., a plurality of different databases ...”);

see also *id.* at 40-41, 44, 47, 49 (emphasis in original). In my opinion, Tajima does not disclose and/or render obvious limitation 1[d].

39. I understand that Petitioner and Dr. Bhattacharjee rely upon Tajima’s teachings regarding the embodiments disclosed in Tajima’s Figures 12 and 13, wherein “information regarding the key that was used for the encryption” is attached to a data fragment; these embodiments do not disclose attaching the key itself:

Fig. 12

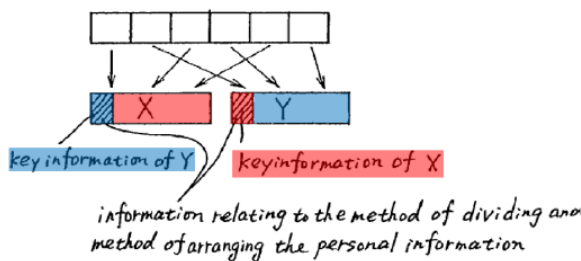
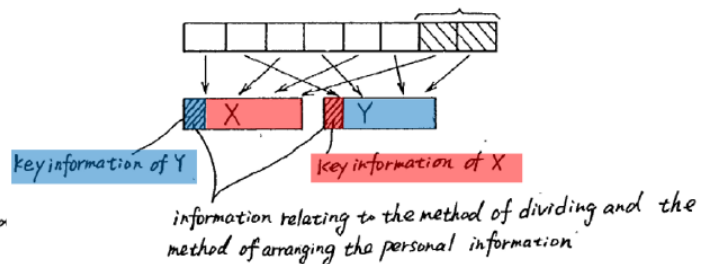


Fig. 13



Pet., 19 (citing EX1005, Figs. 12, 13, [0112]). In particular, Petitioner and Dr. Bhattacharjee argue that “**POSAs understood** that Tajima’s ‘key information’—i.e., ‘information regarding the key that was used for the encryption of [the respective] data fragment’ (EX1005, [0111], [0113])—includes at least the corresponding key for several reasons.” Pet., 20 (citing only EX1003 ¶ 96).

40. It appears that Dr. Bhattacharjee does not contend that Tajima expressly discloses storing a key with the data fragments, but rather contends that Tajima discloses attaching “information regarding the key” to the data fragments

and that a POSITA “understood” this means the key is stored with the data fragments. I disagree with Dr. Bhattacharjee’s assertions of what a POSITA would understand.

41. Petitioner relies on Tajima’s teachings in connection with its Figure 12 and Figure 13 embodiments that “information regarding the key” is stored with the data fragments. I do not believe that a POSITA would understand that Tajima uses the term “information regarding the key” to refer to the key. If Tajima meant to say the “key,” there would be no need to use the phrase “information regarding the key.”

42. When Tajima wishes to refer to a “key,” it does so directly. *E.g.*, EX1005 [0067] (“directory 60 for registering **a public key** that the user of user terminal 10 has registered with certificate authority 40a in advance.”), [0070] (“In Step S1, the user of user terminal 10 first uses user terminal 10 to **create a public key and secret key** ..., and further, submits **this public key** and personal information ... to certificate authority 40a in Step S2.”), [0071] (“Upon receiving **the public key** and personal information in Step S3”); [0075], [0077], [0086] (“the user ... uses **the secret key** that was created in Step S1 (see FIG. 6) to encrypt the compressed permit”), [0088] (“Store 20 then uses **the acquired public key** to check whether the received permit was created by the user”), [0089] (“store 20 first uses **the public key** that was acquired in Step S28 to decrypt the encrypted permit”).

43. Thus, Tajima appears to use the term key when it means a key, and uses the terms “information *regarding* the key” and “key information” to refer to some type of information about the key, not to the key itself.

44. The Petition also asserts that that because “Tajima never says that anything else” about what constitutes key information and “does not disclose” a “separate key management infrastructure,” it must be the case that “the key information includes the key.” Pet., 20-21. But Tajima’s silence does not compel this inference.

45. Petitioner and Dr. Bhattacharjee seem to be relying upon Tajima’s silence regarding key management, arguing that information regarding the key includes the key itself because Tajima “does not disclose any additional steps nor any separate key management infrastructure.” This conclusion does not logically follow. All Tajima discloses is that “information regarding the key” is stored with the data fragment. It is silent about what key information is and where the key itself is stored.

46. Petitioner also relies on Tajima’s statements that “information regarding the key” “is used to decrypt” a data fragment. EX1005 [0112], [0114]. But that does not establish that the key itself is *stored* with the data fragment. If the information regarding the key indicates, *e.g.*, the type of key that is used, or

information that can be used to derive the key, such information could be “used to decrypt” a data fragment without being the key itself.

47. I understand that Petitioner and Dr. Bhattacharjee present an alternative theory that the inclusion of the key itself in key information would be obvious. Pet., 22; EX1003 ¶ 104. But in my opinion, Petitioner offers no evidence or explanation of why attaching the encryption key itself to a data fragment “would have been an obvious and conventional way” to modify Tajima.

48. The inventions-at-issue concern cryptography, which is a technologically-involved and complex field involving incredibly high stakes and safeguarding against a wide variety of highly sophisticated and ever-evolving cybersecurity attacks. Thus, a POSITA would be hesitant to modify existing practices in favor of untested techniques with no history of peer review. See EX2006, 3 (“Few can do the science [of cryptography] properly” and “[g]ood cryptographers know that nothing substitutes for extensive peer review and years of analysis.”).

49. Petitioner’s proposed modification to Tajima involve where and how to store encryption keys and thus cannot be merely “conventional.” Rather, these choices must be carefully considered and the threat model properly assessed because key management is the most difficult and most vulnerable part of cryptography.

See EX2010, 169 (“In the real world, key management is the hardest part of cryptography.”); EX2008 (“And just as it’s possible to build a weak structure using strong materials, it’s possible to build a weak cryptographic system using strong algorithms and protocols.”); EX2009 (new computer “security systems have a nasty habit of backfiring”).

50. As Petitioner and Dr. Bhattacharjee acknowledge, there are significant security drawbacks to including the encryption key itself in the “key information” because “[i]t was known that storing plaintext (*i.e.*, unencrypted) keys with encrypted data results in a vulnerability.” Pet., 33-34; EX1003 ¶¶ 140. To the extent a key might be first encrypted and then stored, that would require management of keys outside of the key information with the fragments contrary to what the Petition asserts as the goal of Tajima, namely “a system that needs only the key information to decrypt data fragments and not additional key management infrastructure.” See Pet., 22.

C. Petitioner’s Tajima/Foster, Tajima/Rivest, and Tajima/Rivest-Shyu Grounds Fail (Grounds 2, 3, and 4; Claims 1-3, 6, 9-14)

51. Claims 2, 9, and 11-14 of the ’116 require “transforming each of the plurality of different encryption keys” which were used to “encrypt[] each of the data chunks.” *E.g.*, EX1001 cl. 9.

52. I understand that Petitioner does not dispute that Tajima does not teach “transforming each of the plurality of different encryption keys” under any parties’ construction.

53. Rather, Petitioner proposes combining Tajima with Foster to allegedly meet Patent Owner’s construction of “transforming” (Pet., 6-7) and Tajima with Rivest to allegedly satisfy Petitioner’s construction of the term (*id.*, 6). Petitioner then adds Shyu to Tajima and Rivest, apparently in order to meet its own construction of “data indicative of at least one of ... the encryption keys.”

1. The Tajima-Foster Ground Fails (Ground 1; Claims 1-2, 9, 11-14).

54. It is my opinion that Tajima and Foster are directed to entirely different fields and different problems. Tajima “relates to a personal information management system” and improves upon a prior art “online shopping system” and prior art “public key cryptosystem” with a certificate authority. *See* EX1005, [0001], [0004]-[0007], [0025], [0042]. Thus, Tajima teaches that “an object of” its invention is to “improve the security of personal information.” *Id.*, 44. More specifically, Tajima addresses “online shopping” wherein “a user purchases goods” and “the payment method[] and the content of the customer information” including “the user’s name, address, telephone number, and e-mail address” must be provided to the store. *Id.*, [0004]-[0007].

55. Tajima discloses a system in which a dataset comprising a user's personal information is divided into multiple "data fragments," which I understand Petitioner contends correspond to the "data chunks" of claim 1. Pet. 15. In the embodiments depicted in Figures 12 and 13 of Tajima, the dataset is divided into at least two fragments, indicated as "X" and "Y" and each is encrypted using a different key."¹ *Id.* 18.

¹ Tajima indicates that the dataset may also be divided into "three or more" fragments. EX1005 [Tajima] 0156].

Fig. 12

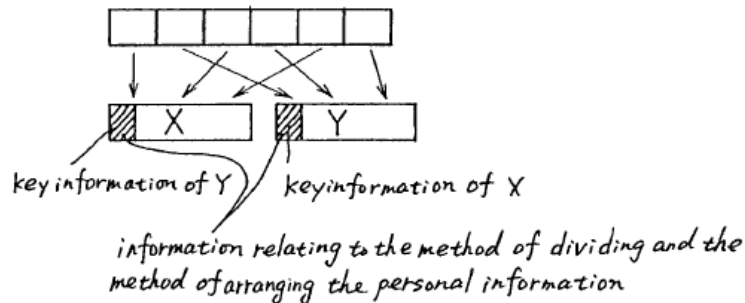
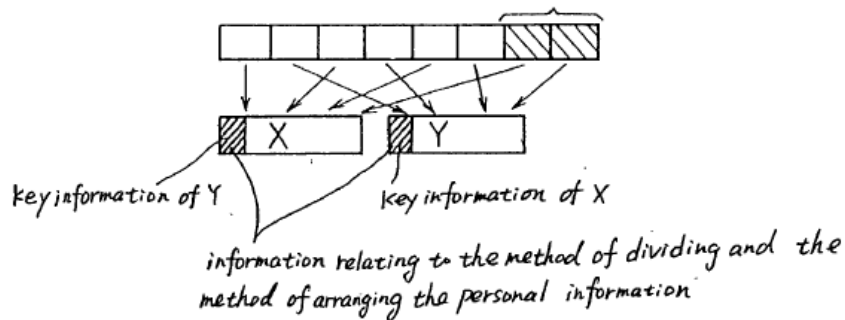


Fig. 13



56. Tajima explains that after they are encrypted, “information regarding the key that was used for the encryption of data fragment Y is attached to encrypted data fragment X, and information regarding the key that was used in the encryption of data fragment X is attached to encrypted data fragment Y.” In other words, each chunk is attached to information about a key that is not the one used to encrypt it. EX1005, [0111]-[0114]. Data fragment X (with the attached key information for another data fragment) is then “registered” (or, the Petition asserts, stored) with a

different certificate authority than fragment Y (likewise, with attached key information for another fragment).

57. Foster, by contrast, is directed towards a system wherein a content owner (e.g., a movie studio) provides content to Foster's system for encryption so that the content can be streamed (e.g., via the internet) to a recipient.

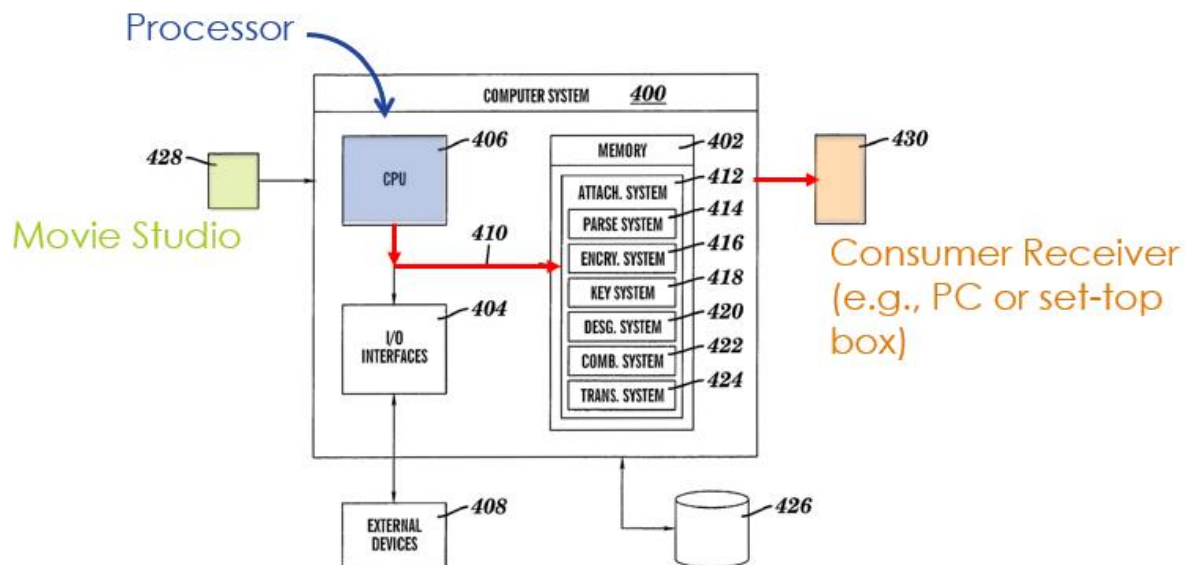


FIG. 16

See EX1006 Fig. 16 (annotated), [0002] (“a method, system and program product for attaching a title key to encrypted content for synchronized transmission to a recipient.”), [0078] (“computer system 400 is intended to be representative of any system capable of processing content units of an elementary content stream received from source 428, and transmitting the processed content units to a recipient 430.”).

58. Foster's teachings of synchronized transmission are primarily significant in a streaming context a stream where player can start [displaying the stream]]”:

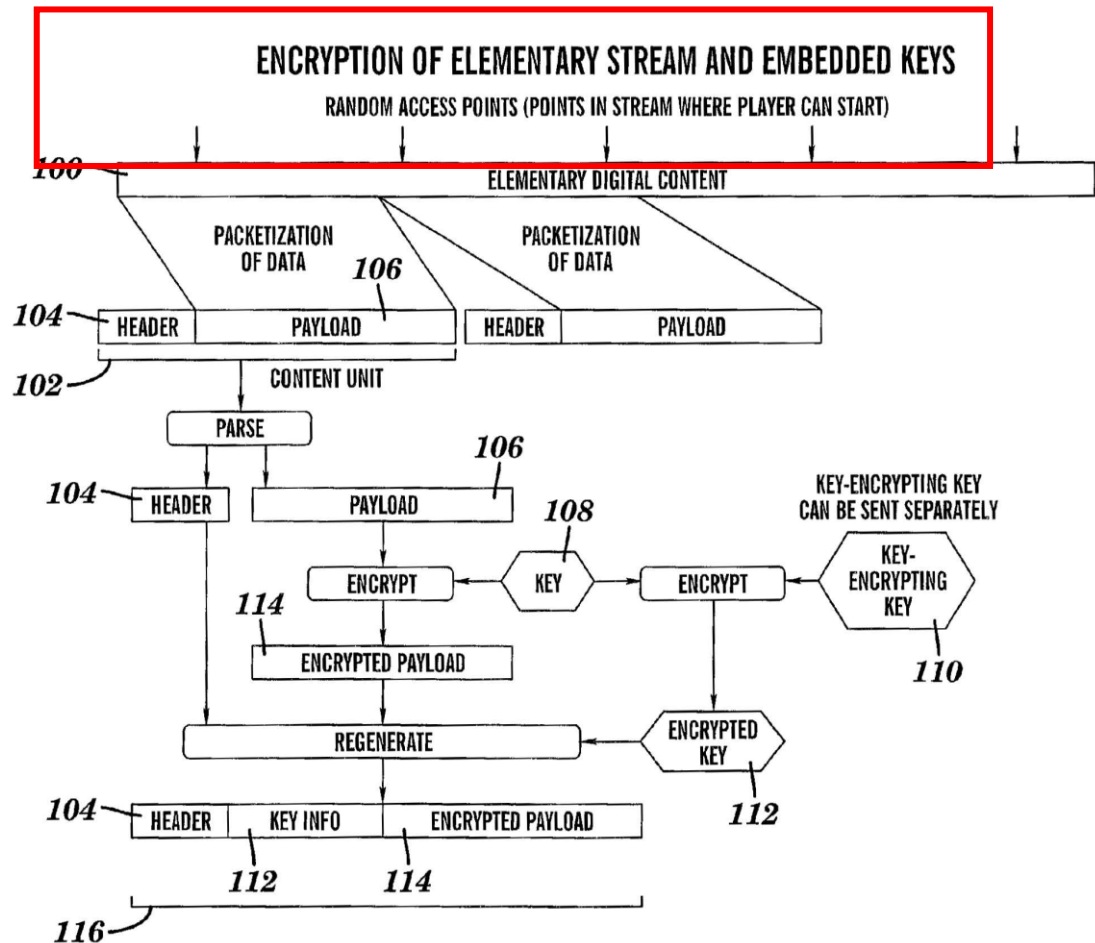


FIG. 8

EX1006 Fig. 8; see also *id.*, [0064].

59. Foster makes clear that when content and keys are not sent synchronously, the type of random access of content contemplated by Figure 8 “is not possible” in the streaming context. *Id.*, [0063]; *see also id.* at [0064], [0071].

60. To facilitate streaming, Foster’s system is ***directed towards synchronizing the transmission of encrypted content packets with the keys used to encrypt those packets***, so that each packet can be viewed as soon as it is received. EX1006, Title (“Method, System and Program Product for Attaching a Title Key to Encrypted Content for Synchronized Transmission to a Recipient”). By “synchronized” transmission, Foster means specifically that the keys used to encrypt the content packets “are ... attached to the corresponding encrypted content packets.” EX1006, Abstract.

61. In contrast to Tajima’s disclosure that its title key is secured by attaching it to a different data fragment, the problem Foster sought to solve is “the need ... for a key used to encrypt content to be itself encrypted, and transmitted as an integral part of the [same] content.” *Id.*, [0007]. Foster purports to solve this problem by doing the opposite of that taught in Tajima—attaching each encryption key to the packet it can decrypt. Foster is designed to improve upon prior art systems that were susceptible to loss of synchronization between the content and the keys.

62. In my opinion, Tajima and Foster are far afield of one another, arise in manifestly different environments and confront quite different problems. I do not believe a POSITA would have naturally combined Tajima and Foster in the normal course of research and development.

63. Petitioner contends that a POSITA would combine Tajima and Foster by using Tajima's disclosure of "dividing personal information and securely storing data fragments on [different] databases" with "Foster's key-encryption technique." Pet., 37-38. More specifically, Petitioner asserts that the combination would "store each data fragment" created by the method of Tajima, with "encrypted key information" that includes the title key (of Tajima) encrypted with a key encryption key according to the method of Foster. The encrypted key information would then be stored with a data fragment other than the one the title key was used to encrypt, as in Tajima. *See* Pet., 45. Petitioner claims that a POSITA "would have recognized the desirability of using Foster's key-encryption technique to encrypt Tajima's keys before attaching them to different encrypted fragments" to benefit from a purported "increased level of security." Pet. 37. Petitioner also claims that the POSITA "would have realized that this benefit would be achieved with little modification to Tajima's system."

64. It is my opinion that combining Tajima and Foster would be neither easy nor beneficial, and a POSITA would not be motivated to make the combination proposed by Petitioner with a reasonable expectation of success.

65. In my opinion, a POSITA would not be motivated to combine Tajima and Foster because they lack key disclosures. Each reference is silent about a key feature of the claimed inventions, so it would be unclear to a POSITA how the claimed inventions could be achieved by combining the references. In addition, applying the key encryption technique of Foster to Tajima's key information would render the technique Tajima already uses to secure that information redundant.

66. While Tajima discloses dividing a dataset into data fragments corresponding to the claimed data chunks, it only discloses attaching "information regarding the key" to those data fragments. Tajima does not disclose attaching the key itself to a data fragment. Meanwhile, Foster operates on MPEG video packet payloads and does not disclose generation of data chunks. Further, Foster requires that the key used to encrypt packets of media content be attached itself to the payload of a media packet.

67. First, It is my understanding that limitations [1A] and [9A] of the '116 Patent require "distributing the data set into a plurality of data chunks." Petitioner maps the claimed "plurality of data chunks" to Tajima's data fragments, and asserts,

as a conclusion, that “like Tajima,” Foster “divides digital content into content units.” Pet., 36. Petitioner, however, fails to show that Foster’s “content units,” which are MPEG video packet payloads, are the claimed “data chunks” or that a POSITA would understand that content units correspond to Tajima’s data fragments.

68. Petitioner and Dr. Bhattacharjee rely on a correspondence between Tajima’s data fragments and Foster’s packet “payloads” as the claimed data chunks. Pet., 36. But Foster teaches that these “payloads” refer to the payloads of MPEG Packetized Elementary Stream (PES) packets (also referred to in Foster as “content units”), as illustrated in Foster’s Figure 13. *See* EX1006, Fig. 13; *see also id.*, [0072] (“a MPEG packetized elementary stream 300 is parceled into PES (packet) units 302 PES unit 302 includes packetized elementary stream (PES) packet payload 306” which “will be encrypted with a title key”). Unlike the “data chunks” described in the ’116, these payloads do not exist to protect the data.

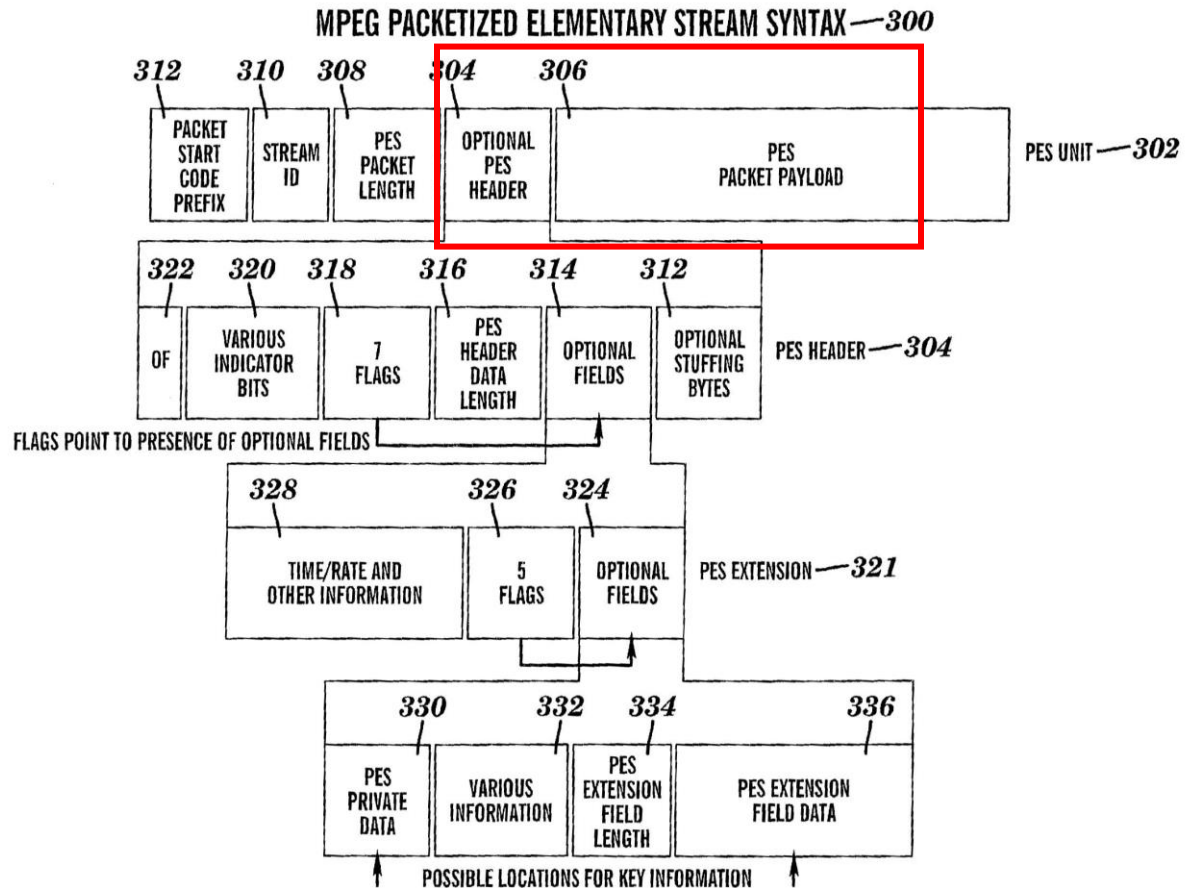


FIG. 13

69. As the '116 explains, partitioning the data set into chunks increases security because when “data ... remains whole and intact,” it is “subject to attack.” The '116 addresses this concern, in part, by “performing a cryptographic parsing and splitting of the encrypted file.” EX1001 57:10-24. Tajima teaches that in order to create the data fragments, a personal information dataset “is first divided into a plurality of data portions each of a predetermined fixed length, and this

plurality of data portions is then arranged as two [or more] data fragments, according to a set method of arranging” to secure the dataset.

70. A packet payload (as in Foster), however, is not created to protect the data. Rather it exists by virtue of the MPEG packetized elementary stream standard. EX1006, [0072]-[0073]; EX2014 (“An elementary stream is broken up into packets, forming a *packetized elementary stream* (PES).”). These packets allow for transmission of the content. See EX2015, 626 (“**Packet** 1. Generic term for a bundle of data, usually in binary form, organized in a specific way *for transmission*.”); EX2016, 257 (“a group of binary digits forming a message. The group is *transmitted* together”).

71. Consistent with the fact that they are not intended to protect data, numerous technical articles refer to a packet or packet payload itself being divided into chunks or fragments. See, e.g., EX2036, 1202 (“The new scheme uses a content-based chunking algorithm to consistently divide both files and packet payloads into multiple byte sequences, called chunks.”); EX 2037, 1 (“These services allow breaking down packet payloads into smaller units (called chunks) ...”); see also *id.*, 2 (“It provides a packetization method that breaks down the payload into multiple chunks, each with a certain significance.”); EX2012, 3 (“[The d]ata packet is delivered as a sequence of chunks.”); EX2013 (“the input is

a large data packet ... which is delivered in small chunks.”); EX2038 4-5 (“A packet consists of multiple chunks...); EX2041, 7 (“the payload could be divided into multiple equal-sized chunks...”).

72. It is my opinion that a POSITA would not be motivated to apply Foster’s disclosures about encrypting the keys used to encrypt the packets of an MPEG video stream for transmission to information regarding the keys (not the keys themselves) used to secure Tajima’s data fragments for storage.

73. The silence of Tajima, on the one hand, about attaching the keys themselves to data fragments, and the lack of disclosure in Foster about anything corresponding to a data fragment, means that a POSITA would not be motivated to combine (and would not have any reasonable expectation that) these references could be successfully combined to achieve the inventions disclosed in independent claims 1 and 9, as these claims require attaching the key itself to a data chunk.

74. Second, it is my opinion that a POSITA would not be motivated to combine Foster to Tajima because Tajima’s key information is already secured by hiding it—by attaching it to a data fragment it cannot decrypt, and storing the different data fragment/key information combinations in different locations. *See, e.g.*, EX1005, [0110]-[1015]. Petitioner acknowledges this, with respect to the only combination it proposes, by stating that “Tajima Foster [] obfuscates keys by

attaching key information to a different data fragment . . . and additionally obfuscates [Tajima's] keys by "encrypting [them] with a KEK [key encryption key]" according to the method of Foster. Pet., 41-42. Applying Foster to secure the key information through encryption would render the method already used by Tajima to secure that information redundant. Neither reference suggests that Tajima's method of hiding the keys fails to provide adequate security, and Foster ties its key encryption method to the need to transfer the title key used to encrypt the packets with the packets themselves.

75. Foster acknowledges that its "title key is encrypted with the key encrypting key" precisely so that it "can then be transmitted along with the encrypted content." EX1006, [0053]. By this suggestion, Foster ties the benefits of its KEK method to the need to secure the keys that encrypt the packets themselves (by encryption with a KEK) so that the keys can be transmitted together with the packets. If the packet encryption keys were not themselves encrypted, they could not be transmitted with the packets, as an attacker with access to the transmission would get both an encrypted packet and an unsecured key that can be used to immediately decrypt it. Tajima, in contrast, has no need to further secure its key information by encryption because it already secures that information by hiding it with a data fragment it cannot decrypt. Thus, an attacker

with access to a system that stores fragments according to Tajima does not have the key information needed to decrypt that fragment.

76. It is my opinion that even if one assumed that (1) the “key information” of Tajima includes the keys used to encrypt its data fragments; and (2) that MPEG packet payloads/content units of Foster correspond to a data fragment, a POSITA still would not be motivated to combine them. Any combination would require eliminating the benefits of both systems to create a system that cannot achieve the objective of either reference. Indeed, Foster discourages a POSITA from adopting the method of Tajima, by emphasizing the efficiency of keeping an encryption key and the packet it can decrypt together, and decrying the disadvantages of attaching an encryption key to a packet it cannot decrypt.

77. In the embodiments of Tajima on which Petitioner relies, depicted in Tajima’s Figures 12 and 13, a dataset is divided into two fragments, X and Y”; each fragment is encrypted using a different key.” *Id.* 18 (citing Tajima EX1005, [0111], [0113]). After data fragments X and Y are encrypted, “information regarding the key that was used for the encryption of data fragment Y is attached to encrypted data fragment X, and information regarding the key that was used in the encryption of data fragment X is attached to encrypted data fragment Y.” In other words, each chunk is attached to, and stored with, information about a key that is not the one

used to encrypt it. Tajima EX1005, [0111]-[0114]. This means that by design Tajima's system cannot perform synchronized transmission.

78. Foster, by contrast, discloses a system in which “[t]he encrypted title key [is] attached to the content packet and the header for synchronized transmission to, or storage by a receiver. *Id.*, [0008] In fact, attaching the key to content it can decrypt for synchronized transmission of the two together is essential to Foster's system—it is “the whole invention,” as Dr. Bhattacharjee opined at his deposition. EX2034, 32:20-23.

79. In the Petition's proposed Tajima/Foster combination, each title key would be attached to a different data fragment than the one it can decrypt, as is done with the key information in Tajima. Pet., 33-34. But a POSITA would not be motivated to do this as it would entirely abandon Foster's “whole invention”—the synchronicity between a packet and the key that can decrypt it.

80. Third, it is my opinion that a POSITA would understand that Foster discourages the combination proposed by Petitioner because it touts the advantages of keeping a key together with the data it can decrypt, and decries the disadvantages of the contrary path in which they are separated (as in Tajima).

81. Foster discloses that in prior art systems, encryption keys were separated from the content they encrypted. This created a problem because when

the key and content are not synchronized by keeping them together, “the incorrect key might be used and the content could not be decrypted.” EX1006, [0007]. As explained in Foster’s specification, Foster’s invention solved this problem because “by transmitting the encrypted key as an integral part of the encrypted content, a receiver would receive the encrypted content as well as all information necessary to decrypt the content in a single stream.” *Id.*

82. It is my opinion that in light of the above, a POSITA would not be motivated to combine Tajima with Foster.

2. A POSITA Would Not Be Motivated to Combine Tajima & Rivest (Ground 3, Claims 9-14)

83. Petitioner and its expert assert that a POSITA would have been motivated to combine Tajima and Rivest, because they “would have recognized the benefit of applying Rivest’s ‘all-or-nothing’ transforms (AoNT) to Tajima’s key information to protect Tajima’s plaintext keys without needing to maintain secret keys.” Pet., 46. The Petition asserts that “Tajima-Rivest applies Rivest’s AoNT using the user’s public key provided to Tajima’s service sites, . . . and thus beneficially avoids using secret keys.”

84. In my opinion, a POSITA would not be motivated to apply Rivest’s AoNT using the user’s public key as Petitioner suggests. Rivest says nothing about the use of public keys and is not designed to be used with public keys.

Rivest is generally used in connection with symmetric encryption systems that require a secret key. Public key encryption systems generally use different types of transformations. Instead of a public key, Rivest requires the use of a random number as the basis for its AoNT transformation. *See* EX1034, 213-14.

85. A POSITA would understand that without and a secret key, Rivest's AoNT provides no security. EX1034, 212. Rather, the AoNT is used because it adds a property to a data set that can be useful for some applications.

86. Rivest discloses that the AoNT is merely a “pre-processing” step “that has certain interesting properties,” but by itself does not provide adequate protection to a dataset (such as the key information of Tajima). EX1034, 212. Specifically, applying the AoNT to a dataset before it is further encrypted or divided into pieces forces an attacker to “decrypt the entire data set before [it] can determine” even one piece of the data set. *Id.*, 210. For example, AoNT is appropriate if one desires to require that a party in a transaction obtain all of the ciphertext before performing a decryption. However, if the data set has merely been transformed using the AoNT, without further encryption or splitting, “anyone” who knows the random number on which the transformation is based can “invert” it to obtain the original dataset. *Id.*, 212. In the Tajima-Rivest combination proposed in the Petition, that number would be a public key that is

known to anyone. Because Tajima does not suggest separately encrypting or parsing its title keys into smaller pieces, in my opinion, a POSITA would not see any benefit in combining it with Rivest's AoNT based on a public key.

87. In my opinion, Petitioner is simply wrong in contending that a POSITA would be motivated to combine Tajima with Rivest "to secure the plaintext keys without the need to maintain secret keys." The AoNT transformation of Rivest cannot secure a key without a further encryption step or fragmentation step that would have to be added to Tajima. See EX1001, 77:5-47. If further encryption is used, that would require the system to use and maintain another secret key. Fragmenting the key and storing the pieces in different locations would be another way of securing the transformed title key, but that also is a step that would have to be added to Tajima that would require maintaining information about the locations of the pieces of the fragmented key.

88. Rivest also points out that "all-or-nothing encryption has **terrible** error-propagation properties" because if any pseudo-message block is damaged "then it is likely that **every** message block will be damaged." EX1034, 216. Accordingly, redundancy information should be included in any data set before it is transformed using the AoNT, a practice that is suggested in the '116 (see 77:23-36) but which would have to be added to Tajima.

89. Tajima is directed to a database for user information. Far from suggesting the use of redundant information, Tajima states that, as to its data fragments, no one fragment is sufficient to recreate the data set. EX1006. Introducing redundancies into such a database could also tax storage space and could slow the processing of user data to the extent required to remove redundant information to efficiently transmit and use the data.

90. It is my opinion that in light of the above, a POSITA would not have been motivated to combine Tajima and Rivest.

3. A POSITA Would Not Have Motivation to Combined Tajima, Rivest, and Shyu (Ground 4; Claims 1-3, 6).

91. The Petition and Dr. Bhattacharjee also assert that that Shyu should be combined with Tajima and Rivest. Pet., 48-50. The Petition suggests that adding Shyu provides the “metadata” Petitioner claims is required to meet its construction of the phrase “data indicative of at least one of the plurality of different encryption keys.” Pet., 48-50.

92. Dr. Bhattacharjee states “[a] POSA would have recognized the benefit of applying different encryption algorithms to different data fragments as taught by Shyu to avoid known security risks of using a fixed encryption algorithm.” EX1003 [Bhattacharjee-Dec.] ¶204. I disagree.

93. In my opinion, **no** POSITA would believe security would be improved by applying different encryption algorithms to different pieces of the same data set (per Shyu) because doing so would violate Kerckhoff's Principle, a long-standing and fundamental tenet of cryptography.

94. Kerckhoff's Principle, first formulated in the late 19th century, is one of the foundational rules of cryptography, taught to every cryptography student as part of their introduction to the field. As formulated by Kerckhoff in the context of military encryption, the rule states that "[t]he cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience." EX2007, 3. In other words, it holds that a cryptosystem should be secure, even if everything about the system, except the key, is public knowledge. *Id.* Stated differently, Kerckhoff's Principle demands that security rely solely on the secrecy of the key. Kerckhoff's Principle has been widely embraced by cryptographers for decades. This stands in stark contrast to their rejection of the notion of "security by obscurity" which is the idea that higher security can be achieved by keeping a cryptographic algorithm obscure (or hidden) from public view. *Id.* There are a number of reasons for Kerckhoff's rule, including that: (1) it is easier to secure a random key than a random algorithm; (2) the number of good encryption algorithms is limited and it is not difficult for an attacker to try all of them; (3) it

ensures that the level of security provided by an encryption system can be mathematically proven, whereas the likelihood that the method behind an *ad hoc* system such as Shyu might be leaked or disclosed cannot be reliably estimated.

95. Shyu's anti-piracy system is a prototypical example of an attempt at security through obscurity, to the extent it proposes to make the system more secure by concealing or obscuring the encryption algorithms (Pet., 48-49) used on any data set or piece of a data set. Because it violates Kerckhoff's Principle, a POSITA would be discouraged from following the path it discloses, much less motivated to combine it with Tajima and Rivest with any expectation of success.

96. Shyu discloses "a data encryption method and system for effectively guarding against piracy of source data during data transmission." EX1016, 1:32-34. Shyu explains that "the object of the present invention is to provide a method and system for dynamic data encryption," in which the encryption algorithm is "dynamically changed to guard against piracy when data is transferred between two entities, such as a transmitter and a receiver of a data processing system." *Id.* 1: 35-41. The goal is to protect against software piracy "**during**" transmission of the software from a transmitter to a receiver. *Id.*, 1:5-10 (emphasis added).

97. It is my opinion that adding dynamic encryption as taught by Shyu provides no benefit to Tajima's system and adds substantial unwanted complexity.

98. Shyu seeks to address the problem of piracy by an attacker during the transmission of a data set in blocks *from a single source to a single destination*. In those circumstances, an attacker watching the transmission has access to all of the transmitted blocks. If the same encryption algorithm is used for every block, the an attacker with access to the transmission only has to correctly ascertain the algorithm once, and can could use that knowledge to decrypt the rest of the entire transmission. But Tajima does not present this risk, because in Tajima *different pieces of the personal information data set are transmitted to different destinations*. There is no reason to dynamically change the encryption method for different data fragments in Tajima, because there is no way for an attacker watching a single transmission to get all of the fragments that comprise the data set.

99. It is my opinion that a POSITA would also not be motivated to combine Shyu with Tajima and Rivest because doing so would add to the system the substantial complexity associated with maintaining multiple encryption algorithms and of tracking encryption algorithm “metadata,” to the system without providing any substantial security benefits.

4. Petitioner's Explanation of Proposed Motivations to Combine Tajima/Foster, Tajima/Rivest and And Tajima/Rivest/Shyu Do Not Consider Drawbacks And Are Purely Hindsight Driven.

100. It is my understanding that an obviousness analysis asks whether a POSITA would have been motivated to combine the teachings of two references at the time of the invention must after considering both the drawbacks and benefits of a proposed prospective combination and that such any motivation to combine cannot be based on hindsight understanding of the success or benefits of the challenged patent.

101. It is my opinion that a POSITA would not have recognized any of Petitioner and Dr. Bhattacharjee's proposed motivations to combine Tajima with Foster, or Rivest or Rivest/Shyu at the time of the '116 alone or with Rivest and Shyu. Dr. Bhattacharjee's motivations to combine Tajima with Foster, Rivest or Rivest/Shyu seem entirely driven by what the claims of the '116 require. Dr. Bhattacharjee first argues that it would be "obvious" to modify Tajima such that the "key information"—which, as I previously explained, does not indicate the explicit inclusion of the encryption key—now includes the encryption key itself. EX1003, ¶102; Pet., 22. Later, however, Petitioner argues that Tajima's (now-modified) teaching of attaching keys to the encrypted data chunks is flawed, making Tajima's system less secure which would, supposedly, motivate a POSITA to turn

to Foster or Rivest to provide methods of securing those attached keys. *Id.*, ¶¶141-59, 184-92. This is creating a problem in order to provide a solution that would satisfy the claims. No such security flaw existed in Tajima before Petitioner’s Dr. Bhattacharjee’s proposed modification of including the encryption keys with the key information. Indeed, applying a key-encryption key or AoNT to “information regarding the key” would do little to improve security. Adopting the solution of “transforming” the keys is a solution that seems driven only by Dr. Bhattacharjee’s proposed modification which created the problem in the first place, not any preexisting technological need or benefit derived from improving upon Tajima’s unaltered teachings.

102. In my opinion Petitioner and Dr. Bhattacharjee tacitly acknowledge they are using the ’116’s disclosure of using AoNT on encryption keys to supply the motivation to combine Tajima and Rivest when they state that:

The ’116 patent itself acknowledges that AoNT was “well-known” and that “it **will** be understood that the AoNT may be applied to encryption keys used to encrypt the data portions following parsing and splitting.” EX1001, 77:13-43; Bhattacharjee, ¶184.

Pet., 47; *see also* Ex. 1001, 77:13-42 (describing inventive methods of applying an AoNT “to further secure data”). This seems to acknowledge that the use of AoNT would be understood by reading the disclosures of the ’116—and conversely, that

would not have been understood from the information available to a POSITA without those disclosures.

103. Shyu appears to be added, not because a POSITA would have been motivated to combine it with Tajima and Rivest—they would not, but based on a result-driven effort to meet a claim limitation under one of the parties’ propose claim constructions.

D. The Foster-Hayhurst Ground Fails (Ground 5; Claims 1-2, 5, 9, and 11).

104. In my opinion, a POSITA working in the field of the ’116, securing data, would not have selected Hayhurst for combination with Foster during normal research and development because Hayhurst is directed to decentralized media which involves fundamentally different objectives than either Foster or the ’116 Patent. Similarly, it is my opinion that a POSITA would not have combined Foster/Hayhurst as proposed.

1. Hayhurst is Not Analogous Art to the ’116 Patent.

a. Hayhurst And The ’116 Patent Do Not Share The Same Field Of Endeavor.

105. As Petitioner and Dr. Bhattacharjee admit, the ’116’s field is securing data while Hayhurst’s is decentralized electronic media delivery. EX1007, 13 (recognizing that “‘one aspect of the present invention’ is a method for securing data

from unauthorized access or use.”); EX1003, ¶ 31 (same); Institution Decision 2-3; Pet., 55 (“Hayhurst concerns ‘electronic media delivery, such as video-on-demand’”); EX1003 ¶ 228 (same); *see also*, EX2029, 101:19-25.

106. It is my understanding that in order to determine the field of endeavor, courts look to various sources including a patent’s title, claim preamble, abstract, “background of invention,” and “field of the invention,” and the function and structure of the claimed inventions.

107. Each of these traditional sources for identifying a field of endeavor uniformly confirm that the ’116’s field is securing data.

The ’116’s Field Is “Securing Data”	
Title	“ secure data parser method and system”
Abstract	“ secure data parser for “ securely storing and communicating data ”
Field of Invention	“ securing data from unauthorized access or use.” EX1001 [’116] 1:21-22.
Background of the Invention	focuses on the need “for ensuring data stored and transmitted ... cannot be read or otherwise compromised ” and seeks “to provide a cryptographic system whose security is user-independent ...” <i>Id.</i> , 1:31-33, 2:36-37.
Summary of the Invention	“one aspect of the present invention is to provide a method for securing virtually any type of data from unauthorized access or use.” <i>Id.</i> , 2:39-41.
Claims	each claim concerns “ securely storing a data set” or “ securing a data set”

108. Hayhurst does not share this field. Hayhurst’s field, per these same traditional sources, is “decentralized media delivery.”

Hayhurst’s Field Is “Decentralized Media Delivery”	
Title	“Decentralized Media Delivery”
Abstract	“A decentralized approach to delivering a media file ...”
Technical Field	“This application relates to the field of electronic media delivery ...” <i>Id.</i> , [0002].
Background of the Invention	Focuses entirely upon delivering movie files. <i>Id.</i> , [0003]-[0004].
Summary of the Invention	“The present invention addresses the problem of prohibitive bandwidth requirements for a content provider in delivering video-on-demand or other large media files .” <i>Id.</i> , [0005].
Specification/Figures	“FIG. 1 is a block diagram of a system adapted for carrying out the decentralized media delivery of the present invention.” <i>Id.</i> , [0012] “FIG. 4 is a flow diagram showing how the decentralized media file delivery of the present invention is carried out.” <i>Id.</i> , [0015]
Claims	each claim concerns “securely storing a data set” or “securing a data set”

109. Hayhurst includes disclosures about the security of the media files to which it is directed. But it is my understanding that art is not analogous merely because it includes disclosures that tangentially relate to the field of the patent at issue, and that even art that is in the same general technological area as the subject patent may not be in the same field of endeavor. While Hayhurst mentions security,

that is not Hayhurst's field of endeavor as established by the traditional sources discussed above. Hayhurst does not teach, for example, that prior art systems did not adequately secure media files, or that its invention addresses a need for more security. EX1007, [0003]-[0005].

110. It is my opinion that its mention of the "secure handling and storage" of these files does not alter or expand its field so far beyond decentralized delivery of media files as to encompass the "securing data" field of the '116 Patent.

b. Hayhurst Is Not Reasonably Pertinent to the Problem the Inventors of the '116 Patent Were Addressing.

111. Hayhurst is not reasonably pertinent to the problem the inventors of the '116 patent were addressing.

112. A comparison establishes that Hayhurst is not reasonably pertinent to the problem the '116's inventors were trying to solve. The '116 is directed towards creating a cryptographic system whose security is user independent, while still supporting mobile users. EX1001, 2:36-38. The '116 is directed towards the "ever-increasing need ... for ensuring data stored and transmitted" to not "be read or otherwise compromised." *Id.*, 1:31-40. The '116 discusses certain prior art methods of securing data and the ways in which those methods may be compromised because they rely upon users. *Id.*, 1:34-40 (deficiencies in login/password systems); 1:54-2:07 (deficiencies in public-key systems that are "highly reliant on the user for

security”), 2:20-32 (deficiencies in biometric systems that “suffer[] from a variety of drawbacks” from user losing/breaking smartcard). Consequently, the ’116 addresses the need “to provide a cryptographic system whose security is user-independent while still supporting mobile users.” EX1001, 2:26-38.

113. Hayhurst, in contrast, is directed towards “address[ing] the prohibitive bandwidth requirements for a content provider associated with delivering video-on-demand or other large media files.” EX1007, [0003, 0005]. Hayhurst explains that “[i]t is usually not economically feasible for the operator of, for example, a cable television (CATV) system (or other content provider) to provide for delivery-on-demand a large number of movie selections to subscribers because such a system requires an extensive amount of bandwidth between the content provider and each of the subscriber units (televisions or other display devices) of the network. *Id.*, [0004].

114. In order to solve this problem, Hayhurst teaches “a system that shifts the bandwidth requirements away from the content provider and to the network of subscriber units.” *Id.* In his declaration and at his deposition, Dr. Bhattacharjee agreed that Hayhurst is directed towards the “problem” of extensive bandwidth associated with providing “delivery-on-demand” media content. EX1003, ¶ 178; EX2034 [Bhattacharjee Dep.], 87:7-13; 92:1-11.

115. The '116, again, addresses eliminating user vulnerabilities in storing sensitive information. Hayhurst, by contrast, addresses the prohibitive bandwidth requirements for video-on-demand from the perspective of the content provider. EX1007, [0003]-[0005].

116. Security is merely an ancillary benefit to Hayhurst's solution of decentralizing content delivery. And, what little Hayhurst has to say about encryption does not suggest that it is directed towards securing data in a manner that is "user-independent." Rather, in Hayhurst's system, a subscriber requests both an encrypted movie and an encryption key. EX1007, [0028], [0030]. While the movie is originally dispersed amongst thousands of subscribers, it is reassembled, along with the key, by a single user. Thus, the security of the data (the movie) is user-dependent.

117. Thus, it is my opinion that Hayhurst is not reasonably pertinent to the problem of the '116 because a POSITA would not have expected to solve a problem with securing data sets in general by considering a reference directed to reducing the bandwidth required to transmit video-on-demand. In my opinion, Hayhurst's tangential remarks regarding the security of media files does not change this analysis.

2. The Petition Fails to Establish Any Motivation to Combine Foster and Hayhurst.

118. It is my opinion that a POSITA would not be motivated to combine the Foster and Hayhurst references, because they are incompatible and have conflicting goals. Foster is directed towards real-time streaming of television and live events; as such, it is concerned with avoiding delays that interfere with immediate access to content (*e.g.*, when a user changes a channel). Hayhurst, by contrast, is directed to reducing the bandwidth required by a content provider in a video-on-demand context, where immediate access is unnecessary and, in fact, impossible. Hayhurst's method shifts the bandwidth burden from the content provider but does so in a fashion that introduces, rather than avoids, delays. A POSITA would not be motivated to combine Hayhurst's decentralized content storage into Foster because doing so would frustrate Foster's goal of avoiding delays, render Foster unsuitable for streaming live television, and make Foster's system less secure. Fundamentally, Petitioner's combination would make Foster's system worse for no discernible benefit.

119. As discussed above, Foster's system is directed towards synchronizing the transmission of encrypted content packets with the keys used to encrypt those packets, so that each packet can be viewed as soon as it is received. This fundamental goal is reflected in Foster's title, abstract, field of the invention,

background of the invention, summary of the invention, and its disclosure generally. EX1006, Title; Abstract, [0002], [0008]. Dr. Bhattacharjee agrees that Foster is directed towards the synchronized transmission of encrypted content with corresponding encryption keys, EX2034, 16:8-12. In fact at his deposition he testified that “synchronous transmission to a receiver [to] foster random access to content” was “the whole invention in Foster,” EX2034, 32:20-23.

120. Foster seeks to improve upon prior art systems that were susceptible to “loss of synchronization between the content and the keys.” *Id.*, [0006]. The lack of synchronization impacted user experience with “inherent latencies” and “delays,” particularly when “providing random access of protected content,” *e.g.*, when the user changes the channel and when the image the new image displays. *Id.*, [0006], [0052] (“because delivery of keys and protected content are non-synchronized in a CAS, certain latencies such as delays are inherent in attempting to gain random access to the content.”), [0056] (without synchronization, “a delay could be incurred between when encrypted content is received and when it [is] accessed (*e.g.*, between when a channel is changed and when an image is displayed).”), [0063] (similar), [0064] (“both DRMS and CAS have inherent latencies (*e.g.*, delays) in providing random access [to] content.”). Foster, moreover, indicates that “synchronous

transmission to ... a receiver fosters random access to the content.” *Id.*, [0007], [0052].

121. Foster processes content into “content unit[s]” consisting of an encrypted content packet and the “title key” used to encrypt the packet. The title key is itself encrypted with a “key-encrypting-key,” or “KEK,” before it is combined with the content packet in a single content unit. EX1006, [0008]. As illustrated in Figure 16 below—which Petitioner and Dr. Bhattacharjee consistently relied upon (53, 65, Ex. 1003 ¶¶247-51)—Foster’s system transmits content units **directly** to **recipient 430** on a one-to-one basis:

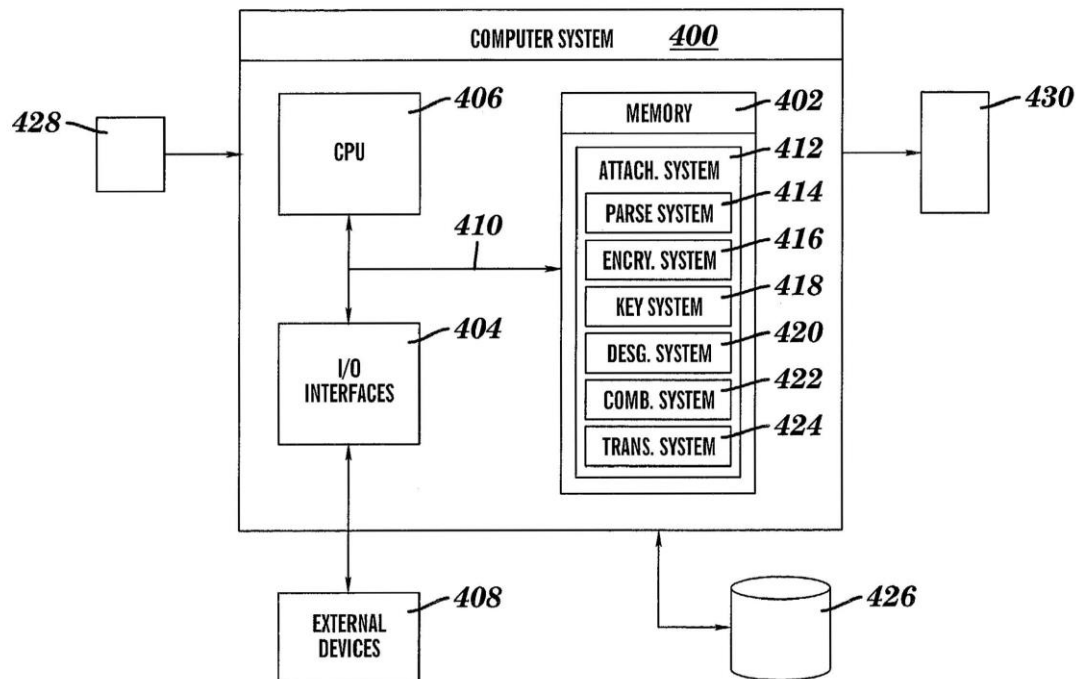


FIG. 16

EX1006 Fig. 16; [0078] (“computer system 400 ... process[es] content units of an elementary content stream received from source 428, and transmit[s] the processed content units to a recipient 430.”). Because each content unit contains both the content and the key, each content unit may be encrypted and transmitted by the source as it is generated, and then decrypted and viewed without delay. *Id.*, [0064].

122. Foster seeks to improve on prior art cable television systems and teaches that its system processes and transmits content units between a “[c]ontent

[s]ervice [p]rovider” “such as a cable service provider” (EX1006, [0039]) and a “[r]eceiver” “such as a set-top box” (EX1006, [0040]). *See also id.*, Fig. 16, [0006] [0052], [0078]. Foster’s teachings of synchronized transmission are primarily significant in a streaming context contemplated by Foster’s Figure 8, which Petitioner relies upon (*e.g.*, Pet., 56, 65-66). “In streaming, multimedia data is transferred in a stream of packets that are interpreted and rendered in real time by a software application, as the packets arrive in the user’s terminal.” EX2035, 220. Because packets are transmitted as a stream and rendered in real-time, any delays have an especially noticeable impact. When watching, *e.g.*, a live sporting event, any delay in receiving, decrypting and/or rendering each content unit in a stream would be a significant drawback. Figure 8 depicts the “Encryption of [an] Elementary Stream,” provided to a set-top box which has “random access points (points in stream where player can start [displaying the stream])”:

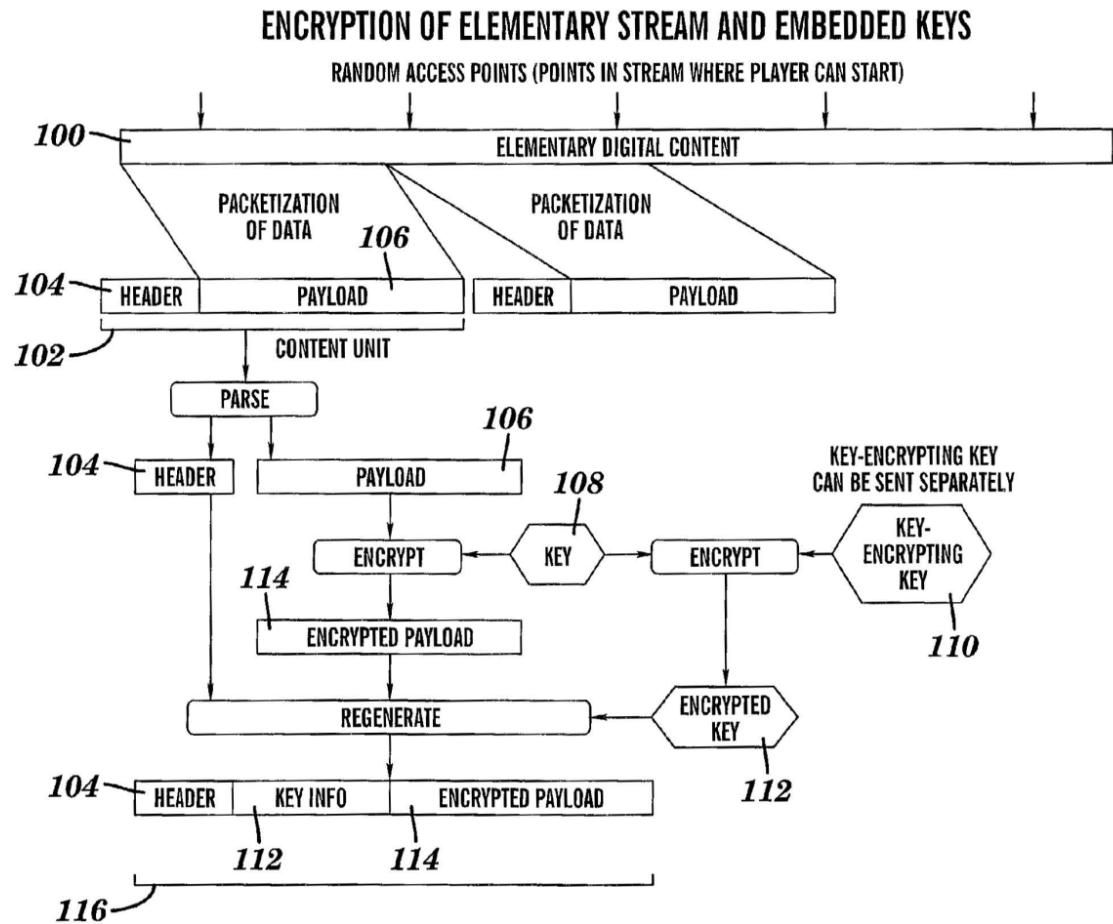


FIG. 8

EX1006 Fig. 8; *id.* [0064]. Foster makes clear that when content and keys are not sent synchronously, the type of random access of content contemplated by Figure 8 “is not possible” in the streaming context. *Id.*, [0063]; *see also* [0064], [0071].

- a. A POSITA Would Not Be Motivated to Combine Because Unlike Foster Hayhurst Is Directed to Reducing the Bandwidth Requirements for the Provision of Content Where Immediate, Random Access Is Not Required.*

123. Hayhurst, by contrast with Foster, is not concerned with synchronous transmission, avoiding delays, or facilitating real-time streaming in any way. Hayhurst purports to facilitate the transmission and playback of content **files**, not content **streams**. Hayhurst's system of first transmitting all pieces of the content and then allowing playback is fundamentally inconsistent with content streaming which allows content to be played simultaneous with the delivery of streaming content.

124. Specifically, Hayhurst aims to overcome "prohibitive bandwidth requirements for a content provider in delivering video-on-demand or other large media files" to a subscriber network. EX1007,[0005]. Hayhurst teaches that, in light of the size of these files and the bandwidth required to transmit them, it is "usually not economically feasible" for a content provider "to provide for delivery-on-demand [of] a large number of movie selections to subscribers." *Id.*, [0004].

125. Hayhurst divides a movie file into segments or packets that are then stored across a network of subscriber units. When a movie is requested by one subscriber, the system directs other subscribers to send their respective segments of the file to the requesting subscriber. When all of the segments are received at the requester's computer, they are then decrypted and the file is reassembled from the

collection of segments for viewing. EX1007, [0006]. Hayhurst's system is a network of "thousands of subscribers." *Id.*, [0016]; EX2034, 101:15-25.

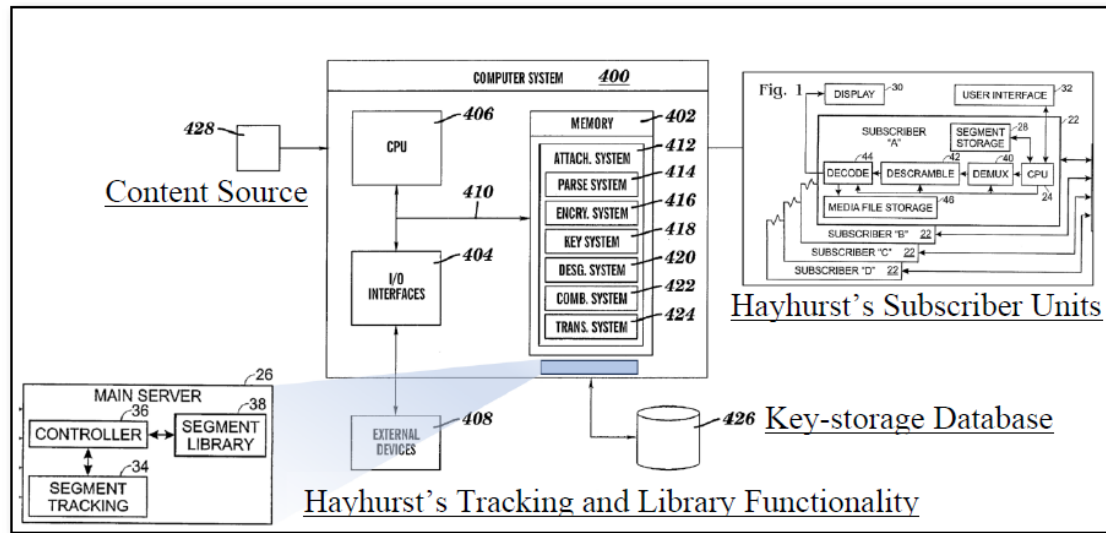
126. Hayhurst's system is not compatible with real-time streaming or random-access viewing of live television. Hayhurst requires that an entire movie file be segmented, and the segments transmitted to, and stored among, the members of a subscriber network before the movie can even be requested for viewing by any individual subscriber. Beyond that, because the segments are not stored in or received in any particular order, the movie cannot be viewed at all by the individual subscriber until (i) **all** segments are received from the subscriber network by the subscriber, (ii) the requesting unit obtains authorization, and (iii) the packets are descrambled and then reassembled into the complete movie file. EX1007, [0029]; [0030]; EX2034, 101:19-25. Thus, Hayhurst's system requires all segments to be received and for the entire file to be reassembled before the system can play the movie. EX1007, [0020].

127. Others in the field have recognized that in "download and play," systems such as Hayhurst "the client has to download and store first **the whole media content** on his PC and only then he/she will be able to view and use it." EX2035 [Patrikakis] 219. This requirement "**exclud[es] the use [of such systems] for**

covering live events, as the multimedia information that is to be transmitted cannot be ‘a-priori’ available.” *Id.*

b. The Combination Involves Storing and Distributing All of Foster’s Content Units per Hayhurst’s Method.

128. It is my understanding that Petitioner posits a combination of Foster and Hayhurst in which Foster’s media **content units** are transmitted and then stored in Hayhurst’s decentralized media **file** storage system. Specifically, “Foster’s encrypted content units” would be stored “on multiple storage devices based on Hayhurst’s techniques for storing and distributing encrypted data segments” of a media file. Pet., 71. In Petitioner’s “exemplary implementation of Foster-Hayhurst,” illustrated below, “Foster’s ‘computer system 400’ is augmented to control distribution of and access to Foster’s encrypted content portions on [Hayhurst’s] ‘subscriber units.’” *Id.*, 65.



Foster-Hayhurst (exemplary implementation)

129. Thus, in Petitioner's combination, Foster's "content stream 100" "is parceled into content units 102" (*id.*, 52) and rather than sending content units directly to the requesting subscriber, the content units would be distributed amongst Hayhurst's network of thousands of subscribers. *Id.*, 64; 62 ("POSAs would have recognized several benefits in storing Foster's encrypted content units distributed on different storage devices as Hayhurst teaches."); 63 (similar); 64 (similar). At his deposition, I understand that Dr. Bhattacharjee admitted that this "is the only implementation of the combination that is described or relied on in the Petition. EX2034, 126:3-9.

c. A POSITA Would Not Be Motivated To Combine Foster And Hayhurst As Proposed in the Petition Because It Would Abandon Foster's "Whole Invention."

130. It is my understanding that in evaluating a POSITA's motivation to make a combination, both the benefits and drawbacks of the combination must be considered. It is also my understanding that a POSITA would not be motivated to combine references where the combination would render the reference inoperable for its intended purpose or to change its principle of operation.

131. In my opinion, a POSITA would not be motivated to combine Foster and Hayhurst as Petitioner proposes because, far from providing any significant benefit, the proposed combination because Petitioner's combination of Foster/Hayhurst would thwart Foster's goals, make Foster inoperable for its intended purpose, synchronized, efficient transmission and random access to content, and compromise any security benefits otherwise provided by Foster alone. Petitioner's combination suffers from three critical flaws. *First*, the combination would introduce the specific delays Foster is designed to avoid, making the synchronization that is the primary purpose of Foster unnecessary. *Second*, the combination would not be capable of providing streaming (*e.g.*, real-time television) or random access to content, contravening Foster's intended purpose. *Third*, the combination would

reduce security as compared to Foster by exposing Foster's key-encryption keys. The Petition does not address any of these issues.

i. Adding Hayhurst's Delivery Method to Foster's System Exacerbates the Underlying Problem Of Delay Foster Seeks to Solve.

132. As explained above, in Foster's system, because each packet in an elementary content stream can be generated as the content is created, and then sent directly to the recipient with its title encryption key, each packet can be viewed without delay, allowing for immediate, random access to the content.

133. Petitioner's Foster/Hayhurst combination would result in inevitable, significant, and crippling delays, the very thing Foster was intended to avoid. Petitioner's proposed combination of Foster and Hayhurst relies upon Hayhurst's methods of storing and delivering segments of media files. Pet., 64. In Petitioner's proposed combination, all of Foster's encrypted content units would, rather than be sent directly to the requestor as in Foster, instead be distributed across thousands of subscriber units before they are then, when requested, sent to a requesting unit, as taught in Hayhurst. EX1007, [0016].

134. This introduces delay in a number of ways. First, in Hayhurst the content must exist as a discrete file before it can be divided into segments and distributed for storage among the subscriber network. (This is in stark contrast to

Foster, where the content units can be created and transmitted as the stream of content is generated.) Then, in Hayhurst, the main server, upon receiving a request, must direct the thousands of subscribers to send segments to the requestor. *Id.*, [0028] (“after the main server receives a movie request 104 from a requesting subscriber..., the server responds 106 by sending over the network instructions to the network subscriber units to direct all of the segments of the requested movie to the requesting subscriber.”). Should there be one or more missing packets, which there inevitably would be for subscribers whose systems are turned off, internet is down, are no longer subscribers, etc., the main server must either direct another subscriber with the same packet to resend it or redistribute the packet. *See id.*, [0025] (“Each segment [] is copied and distributed to a plurality of different subscribers to provide for redundant availability of each segment in the event a subscriber’s segment storage 28 becomes inaccessible. As noted, the main server’s segment-tracking module 34 can ... facilitate replacement or redistribution of segments when necessary.”); EX2029, 106:17-109:6. Accordingly, the requesting unit must wait until “**all** packets are received” before sending a request to the main server to decrypt the segments and reassemble the movie file. EX1007, [0029] (“The subscriber unit CPU 24 and associated buffers (not shown) log the received packets and, once **all packets** are received, sends a notice to the main server 26 that **all packets** now reside

in the unit of the requesting subscriber.”). Only after all of the packets are on the requesting unit does the main server “transmit[] authorization.” *Id.*, [0029]. After obtaining authorization, the receiving unit may descramble, process, and reassemble the entire media file for playback. *Id.*, [0029]-[0030]; EX2034, 109:8-111:1. Only after all of these steps are completed, the movie can be viewed.

135. Consequently, Hayhurst’s methods of storing and delivering content make playback delays—the underlying problem Foster seeks to address—exponentially worse. Rather than immediately streaming content in packets that are synchronized with the encryption keys as Foster does, Petitioner would have Foster’s system store and deliver content using Hayhurst’s decentralized, time-consuming method. In other words, Petitioner proposes changing Foster’s method which has been designed to reduce delays to one that prioritizes bandwidth at the expense of creating delays.

136. In my opinion, a POSITA would not be motivated to change Foster to implement methods which greatly exacerbate the underlying problem Foster seeks to address.

ii. Hayhurst’s Delivery Method Is Incompatible with Foster’s System.

137. The principal application for Foster’s method is real-time cable television broadcasting to a set-top box, therefore, In addition, it is my opinion that

Hayhurst's delivery method is incompatible with Foster's system. Foster's system serves as an intermediary between "source 428" and "recipient 430," where the "source" includes "a cable service provider" (EX1006, [0039], [0042]) and the "recipient" includes a "set-top box" (*id.*, [0040], [0041]). As Dr. Bhattacharjee agrees, Foster specifically seeks to improve upon the "Conditional Access System (CAS)," "such as a cable or satellite television system." *See id.*, [0052]; EX2034, 41:10-15, 30:8-10. Consequently, Foster's principle of operation concerns delivering live cable television to a set-top box. EX2039, (CAS used for OTT digital video streaming service, "such as live sports"); EX2035, (CAS used for "content [transmitted] as a signal, which virtually anyone can pick up via satellite, terrestrial, or cable network."); *see* EX1006, [0056] (Foster seeks to avoid delays "when a channel is changed"); *see also* EX2034, 37:11-39:9.

138. Foster's system is able to deliver live or real-time content as required for cable television because Foster's methods do not require a user to have an entire media file before it can view content. Rather, Foster's system allows viewers to receive and process packets in real-time as they are generated and sent by the content provider. EX1006, [0065] ("the teachings of the present invention can be applied to the scenario where the content is received as content units"); EX2035 [Patrikakis] 220EX2030, 220 ("In streaming, multimedia data is transferred in a stream of

packets that are *interpreted and rendered in real time* by a software application, *as the packets arrive in the user's terminal.*" As a result, Foster avoids "delay[s]" "between when encrypted content is received and when it [is] accessed (*e.g.*, between when a channel is changed and when an image is displayed)." *Id.*, [0056].

139. I note that Petitioner contends that "POSAs had reason to store Foster's encrypted content units on multiple storage devices (*e.g.*, consumer set-top boxes like Hayhurst's subscriber units and Foster's recipients 430)" among the various subscribers in Hayhurst's subscriber network. Pet., 62. But it is my opinion that doing so would render the combination inoperable for viewing streamed content, Foster's intended purpose, because Hayhurst requires, that all segments be delivered to a requesting unit before the content can be reassembled and playback can begin.

140. Hayhurst is directed toward delivering video-on-demand and not live television. In particular, Hayhurst's focus is upon delivering movies—*i.e.*, an already defined media file—in a fashion that avoids bandwidth limitations. EX1007, [0003]-[0004]. As such, Hayhurst can utilize a decentralized delivery system in which segments of a movie are stored on set-top boxes throughout Hayhurst's system until one set-top box requests the entire movie. *Id.*, Abstract, [0006], [0028]. When a requesting set top box requests a movie, it cannot be played immediately. Rather, viewing can only begin after all segments are received, because "the

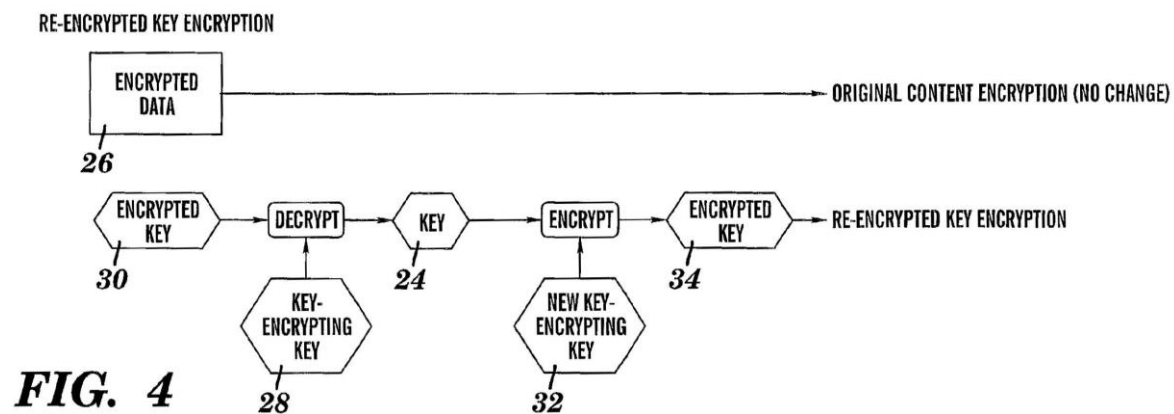
segments are separate in the sense that they represent discontinuous or non-sequential portions of the movie and must be soiled and integrated with the remaining segments (distributed elsewhere in the network) to provide the complete movie.” EX2034, 104:2-13. There is no indication in Hayhurst that the segments arrive in order to the requesting unit. Nor would it be feasible for Hayhurst’s main server to facilitate such a thing, as there would be significant delays incurred as the main server would have to ensure successfully receipt of each segment before directing the next subscribing to send to following segment. Thus, only after all segments are received from the different members of the subscriber network can authorization to decode them be sought and obtained, and the segments are assembled and processed. *Id.*, [0028]-[0030].

141. In the Foster/Hayhurst combination, a set-top box requesting cable television content would have to wait to receive all of the packets sent from the set-top boxes of a multitude of other subscribers before seeking and obtaining authorization and before reassembling and processing the entire content file. This wait-and-see approach would not work when trying to watch live television. EX1006, [0063].

iii. Hayhurst's Methods Make Foster's System Less Secure.

142. In addition, Hayhurst's methods make Foster's system less secure. Foster's content units are encrypted with title keys which are, in turn, encrypted with a key-encrypting-key ("KEK"). Pet., 65-66. In Petitioner's proposed Foster/Hayhurst combination, the encrypted content units would be, as in Hayhurst, distributed across thousands of subscribers. *Id.* A POSITA would not be motivated to do this because it would compromise the security of the system, as compared to Foster, by making Foster's KEKs more vulnerable while eliminating the ability (as disclosed in Foster) to change the KEK as necessary, which is a security benefit of Foster.

143. In Foster, should a key-encrypting-key be compromised or "protection on the content [need] to be varied," "an encrypted title key 30 can be re-encrypted with a different key encrypting key 32 without having to re-encrypt the encrypted content 26." EX1006, [0054].



Id., Fig. 4.

Thus, Foster contemplates seamlessly switching the KEK for security purposes without re-encrypting the underlying content. Thus, if a key-encrypting-key is compromised, or a switch is otherwise desirable, a new KEK may be utilized going forward.

144. Moreover, Foster allows for a KEK to be unique to each recipient. Foster teaches that “key encrypting key 28 is generally determined based on a key management block (KMB), which is typically delivered to a recipient concurrently with or prior to the delivery of encrypted content 26.” *Id.*, [0054]. Because each recipient receives a KMB from which a KEK can be determined, that KEK can be unique to each recipient. This further increases the security of Foster’s content as the damage from any compromise of a recipient’s KEK can be limited to that

recipient and further prevented by simply changing that recipient's key-encrypting-key.

145. Foster/Hayhurst uses Hayhurst's method of storing and distributing content. Consequently, any subscriber (of thousands) is able to request content that has been divided into segments across thousands of subscribers. Because any one of Hayhurst's subscribers can request the content, which has already been segmented and divided in advance, in any combination Foster's content units would all have to be secured using the same KEK(s), regardless of which subscriber will eventually request the content.

146. This, however, makes the combined system less secure for two reasons. *First*, it makes the KEKs more vulnerable. Because the KEK(s) is/are distributed amongst thousands of subscribers, there are thousands of potential points of failure. And, if one set-top-box (of thousands) with the KEK(s) gets compromised, all of the content is compromised because all of the content is encrypted using the same KEK(s) and title keys. *Second*, it would be more complicated to switch KEKs than in Foster alone as all of the content units are distributed across the subscribers instead of streamed in real time as in Foster. Thus, adding Hayhurst's methods to Foster's system would make Foster's system less secure in contravention of Foster's aims.

EX1006, [0004] (“In transmitting such content, however, the security thereof must be ensured.”).

**iv. The Drawbacks Of The Proposed Combination
Outweigh the Claimed Benefits.**

147. Petitioner argues that a POSITA would be motivated to combine Foster and Hayhurst as proposed because Hayhurst’s methods would reduce bandwidth requirements, provide more security, and support redundancy. Pet., 62-63. Petitioner also argues that Hayhurst’s methods result in aggregate speed and efficiency/intelligence. *Id.*, 63.

148. Foster’s system, however, has no need for any of these alleged benefits. Foster’s system simply processes content and transmits streamed content to a particular recipient. EX1006, Fig. 16; [0078]. Because Foster’s system focuses upon streamed content (or content stored on a DVD), and provides a one-to-one transmission from Foster’s system to a particular recipient, there is no indication that Foster’s system suffers from the bandwidth constraints confronted by Hayhurst’s video-on-demand system. Foster’s system, moreover, has sufficient security at the source, security which would be undermined in the combination, as discussed previously. Further, Foster’s system has no need for redundancy as Foster’s system can simply resend dropped packets, nor any need for efficiency/intelligence when sending on a one-to-one basis.

149. Moreover, any benefits are easily outweighed by the drawbacks. Again, Foster is directed towards reducing delays, particularly delays frustrating random access to content. The Foster/Hayhurst combination, however, would introduce enormous delays preventing random access to content and rendering Foster's system unsuitable for streaming live television. Further, the combination would also decrease Foster's security by exposing KEKs and hindering Foster's ability to replace a KEK when desirable.

150. It is my opinion that a POSITA reviewing these references would have been discouraged from making this combination because these manifold drawbacks greatly outweigh any of the purported benefits. For this additional reason, it is my opinion that a POSITA would not be motivated to combine Foster/Hayhurst as proposed.

VII. CONCLUSION

151. Although my complete opinions are set forth above, for convenience I summarize several points of my opinions in conclusion. For the foregoing reasons, based on my expertise and experience and the record of this case that I have reviewed, it is my opinion that:

- Claims 1, 5-8 are not anticipated and/or obvious over Tajima;
- Claims 1-2, 9, 11-14 are not obvious over Tajima and Foster;

- Claims 9-14 are not obvious over Tajima and Rivest;
- Claims 1-3, 6 are not obvious over Tajima, Rivest, and Shyu;
- Claims 1-2, 5, 9, 11 are not obvious over Foster and Hayhurst.

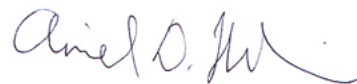
152. I understand that my opinions discussed above support a legal conclusion that claims 1-14 are nonobvious.

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.

I hereby declare that all statements made herein of my own knowledge are true and all statements made herein on information and belief were and are believed by me to be true, and that all statements herein were and are 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 and that any such willful false statements may jeopardize the validity of the application or any patents issued thereon.

Respectfully submitted,

Dated: September 12, 2024

A handwritten signature in blue ink, appearing to read "Aviel D. Rubin", is written above a horizontal line.

Aviel D. Rubin, Ph.D.

Appendix I: Materials Considered

Petition for Inter Partes Review	Paper 2
U.S. Patent No. 11,178,116 (“116 patent”)	EX1001
Prosecution History of U.S. Patent No. 11,178,116	EX1002
Declaration of Samrat Bhattacharjee, Ph.D.	EX1003
Curriculum Vitae of Samrat Bhattacharjee, Ph.D.	EX1004
U.S. Patent Application Publication 2003/0028493 (“Tajima”)	EX1005
U.S. Patent Application Publication 2003/0200176A1 (“Foster”)	EX1006
International Application Publication WO 2004/008289A2 (“Hayhurst”)	EX1007
U.S. Provisional Application 60/396357 (“Hayhurst-Provisional”)	EX1008
Coversheet of U.S. Provisional Application 60/396357	EX1009
Application Data for Provisional Application 60/396357	EX1010
SFI’s 2023-08-14 Infringement Contentions, Chart A	EX1011
SFI’s 2023-08-14 Infringement Contentions, Chart C	EX1012
U.S. Patent Application Publication 2004/0049687 (“Orsini”)	EX1013
International Application Publication WO 2001/22322 (“Dickinson”)	EX1014
U.S. Patent No. 10,452,854 (“854 patent”)	EX1015
U.S. Patent No. 6,021,391 (“Shyu”)	EX1016
U.S. Patent Application Publication 2004/0049700 (“Yoshida”)	EX1017
U.S. Patent Application Publication 2004/0003272A1 (“Bantz”)	EX1018
International Application Publication WO 2001/015162A2 (“Benaloh”)	EX1019
U.S. Patent Application Publication 2002/0194209 (“Bolosky”)	EX1020
U.S. Patent No. 6,819,766 (“Weidong”)	EX1021
U.S. Patent No. 4,238,853 (“Ehrsam”)	EX1022
U.S. Patent No. 7,277,941 (“Ignatius”)	EX1023
U.S. Patent Application Publication 2005/0216754 (“Ehud”)	EX1024
International Application Publication WO 2004/057461A2 (“Ogihara”)	EX1025
U.S. Patent No. 7,178,033 (“Garcia”)	EX1026

U.S. Patent No. 6,490,353 (“Tan”)	EX1027
U.S. Patent Application Publication No. 2006/0064386 (“Marking”).	EX1028
U.S. Patent No. 7,529,834 (“Birrell”)	EX1029
U.S. Patent Application Publication 2001/0037474A1 (“Steegmans”)	EX1030
U.S. Patent Application Publication 2004/0172476A1 (“Chapweske”)	EX1031
U.S. Patent No. 7,099,994 (“Thayer”)	EX1032
U.S. Patent No. 6,151,659 (“Solomon”)	EX1033
Rivest, Proc. Of the 4th Intl. Workshop on Fast Software Encryption 1997	EX1034
U.S. Patent No. 6,308,277 (“Vaeth”)	EX1035
U.S. Patent Application Publication 2001/0053221A1 (“Takeda”)	EX1036
SFI’s 2023-08-14 Infringement Contentions, Chart D	EX1037
Rule 16(b) Scheduling Order, 2:23-cv-00097-JWK-RJK, Dkt. 54 (July 20, 2023)	EX1038
U.S. Patent Application Publication 2018/0367509A1 (“’116 Publication”)	EX1039
ABS: The Apportioned Backup System (“Cooley”)	EX1040
U.S. Patent Application Publication 2003/0081790A1 (“Kallahalla”)	EX1041
Google LLC’s Proposed Claim Terms for Construction	EX1042
Letter from A. Mayron to D. Perlson re Preliminary Proposed Constructions	EX1043
U.S. Patent No. 9,338,140 (“’140 patent”)	EX1044
Bruce Schneier Curriculum Vitae [Schneier-CV]	EX2005
Bruce Schneier, <i>Why Cryptography Is Harder Than It Looks</i> , Schneier on Security, 1997, https://www.schneier.com/essays/archives/1997/01/why_cryptography_is.html [Schneier-Why-Cryptography-Is-Harder-Than-It-Looks]	EX2006
Excerpts from Jonathan Katz et al., <i>Introduction to Modern Cryptography</i> (1st ed. 2007) [Katz]	EX2007
Bruce Schneier, <i>Security Pitfalls in Cryptography</i> , Schneier on Security, 1998,	EX2008

https://www.schneier.com/essays/archives/1998/01/security_pitfalls_in.html [Schneier-Security-Pitfalls-in-Cryptography]	
Excerpts from Ross Anderson, <i>Security Engineering: A Guide to Building Dependable Distributed Systems</i> (1st ed. 2001) [Anderson]	EX2009
Excerpts from Bruce Schneier, <i>Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C</i> (2nd ed. 2015) [Schneier-Applied-Cryptography]	EX2010
Patent Application Publication to Tsai US 2005/0195857 A1 [Tsai]	EX2011
Edgar Pek et al., <i>Formal Verification of Communication Protocols in Distributed Systems</i> , Symposium on Operating Sys. Principles, 2003 [Pek]	EX2012
Jan Friso Groote et al., <i>A Bounded Retransmission Protocol for Large Data Packets: A Case Study in Computer Checked Algebraic Verification</i> , 1996 [Groote]	EX2013
Microsoft, Overview of MPEG-2 Systems, www.learn.microsoft.com , July 27, 2023, https://learn.microsoft.com/en-us/windows/win32/directshow/overview-of-mpeg-2-systems [Overview-of-MPEG-2-Systems]	EX2014
Excerpts from Harry Newton, <i>Newton's Telecom Dictionary</i> (16th ed. 2000) [Newton's-Telecom-Dictionary]	EX2015
Excerpts from Oxford Dictionary of Computing (1996) [Oxford-Dictionary-of-Computing]	EX2016
IBM, Transmission Control Protocol (TCP), www.ibm.com , https://www.ibm.com/docs/en/zos-basic-skills?topic=4-transmission-control-protocol-tcp [IBM]	EX2017
Security First Innovations, LLC v. Google LLC, 2:23-cv-00091 (JKW-RJK), Google's Opening Claim Construction Brief (December 6, 2023) [Google's-Opening-Claim-Construction-Brief]	EX2018
Excerpts from Microsoft Press, <i>Microsoft Computer Dictionary</i> (5th ed. 2002) [Microsoft-Computer-Dictionary]	EX2019

Security First Innovations, LLC v. Google LLC, 2:23-cv-00091 (JKW-RJK), Google's Responsive Claim Construction Brief (Jan. 8, 2024) (Non-Confidential Redacted Version) [Google-Responsive-Claim-Construction-Brief]	EX2020
Cambridge Dictionary, Set-Top Box, https://dictionary.cambridge.org/us/dictionary/english/set-top-box (last visited Feb. 27, 2024)	EX2021
Jim Connors, InfoWorld, The evolution of cable television to interactive communications service provider (Oct. 1, 1996), https://www.infoworld.com/article/2077255/the-evolution-of-cable-television-to-interactive-communications-service-provider.html [InfoWorld]	EX2022
Excerpts from Oxford University Press, Oxford English Dictionary (12th ed. 2012) [Oxford-English-Dictionary]	EX2023
Excerpts from HarperCollins Publishers, English Dictionary for Advanced Learners (3d ed. 2001) [Collins-Dictionary]	EX2024
Japanese Patent Application Publication No. JP2003046500A to Tajima et al. [Tajima-Japan-Application]	EX2025
Cambridge Dictionary, 登録, https://dictionary.cambridge.org/us/dictionary/japaneseenglish/%E7%99%B%E9%8C%B2 (last visited Mar. 22, 2024) [Cambridge-Japanese-English-Dictionary]	EX2026
TechTarget, Certificate Authority, https://www.techtarget.com/searchsecurity/definition/certificateauthority (last updated Sept. 2021) [TechTarget]	EX2027
Declaration of Colette Woo [SERVED, NOT FILED]	EX2028
Jonathan Katz et al., <i>Introduction to Modern Cryptography</i> (1st ed. 2007) [SERVED, NOT FILED]	EX2029

Cambridge Japanese English Dictionary, 登録, https://dictionary.cambridge.org/us/dictionary/japanese-english/%E7%99%BB%E9%8C%B2 (last visited Mar. 5, 2024)	EX2030
Ross Anderson, <i>Security Engineering: A Guide to Building Dependable Distributed Systems</i> (1st ed. 2001) [SERVED, NOT FILED]	EX2031
Bruce Schneier, <i>Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C</i> (2nd ed. 2015) (E-Book) [SERVED, NOT FILED]	EX2032
Deposition Transcript of Dr. Samrat Bhattacharjee, taken on August 9, 2024 [Bhattacharjee-Depo.]	EX2034
C. Patrikakis et al., <i>Streaming Content Wars: Download and Play Strikes Back</i> , UCMedia 2009, LNICST 40, pp. 218–226, 2010. [Patrikakis]	EX2035
J. Hur et al., <i>Packet Chunking for File Detection</i> , IEEE/ACM Transactions on Networking Vol. 31 (2023). [Hur]	EX2036
R. Li et al., <i>A Framework for Qualitative Communications Using Big Packet Protocol</i> , 2019, https://doi.org/10.48550/arXiv.1906.10766 . [Li]	EX2037
N. McKeown et al., <i>The Tiny Tera: A Packet Switch Core</i> , IEEE Micro 17, 1998. [McKeown].	EX2038
<i>Marlin DRM FAQ</i> , Marlin Community, https://www.marlin-community.com/faq/ (last accessed Sept. 9, 2024) [Marlin-DRM].	EX2039
<i>What is Conditional Access?</i> , Verimatrix anti-piracy (Aug. 1, 2023), https://www.verimatrix.com/anti-piracy/knowledge-base/what-is-conditional-access/ [Verimatrix].	EX2040
R. Li et al., <i>New IP: A Data Packet Framework to Evolve the Internet</i> , 2020, https://www.researchgate.net/publication/341582478 [Li-II]	EX 2041

EXHIBIT A

Aviel D. Rubin, Ph.D.

Professor Emeritus, Johns Hopkins University
Chief Scientist & Founder, Harbor Labs

avirubin@gmail.com

<https://www.linkedin.com/in/avirubin/>



Overview

Avi Rubin is a Computer Scientist with almost a decade of industry experience followed by over 20 years in academia. After receiving his Ph.D. in Computer Science from the University of Michigan in 1994, Dr. Rubin worked as a researcher at Bellcore and then at AT&T Labs. In 2003, he joined the Computer Science faculty at Johns Hopkins University and was promoted to Full Professor with Tenure in 2004. During his over 20 years at Johns Hopkins, Dr. Rubin was Technical Director of the JHU Information Security Institute, along with his regular faculty position. In 2023, he was appointed Computer Science Professor Emeritus at Johns Hopkins and joined Harbor Labs, a company he founded in 2011, as Chief Scientist. Dr. Rubin is a frequent keynote speaker at industry and academic conferences and delivered widely viewed TED talks in 2011 and 2015. He has testified about information and network security before Congress on multiple occasions and frequently testifies as an expert witness in Federal court. His awards include Fulbright Scholar, Baltimorean of the Year, and the EFF Pioneer Award.

Academic Degrees

- 1994, **Ph.D.**, Computer Science and Engineering, University of Michigan, Ann Arbor
- 1991, **M.S.E.**, Computer Science and Engineering, University of Michigan, Ann Arbor
- 1989, **B.S.**, Computer Science (Honors), University of Michigan, Ann Arbor

Academic Appointments

September, 2023 - present

Professor Emeritus, Johns Hopkins University

April, 2004 - August, 2023

Professor (with tenure), Johns Hopkins University

August, 2010 - July, 2011

Visiting Research Professor, Fulbright Scholar, Tel Aviv University, Israel

January, 2003 - April, 2004

Associate Professor, Johns Hopkins University

January, 2003 - August, 2023

Technical Director, Johns Hopkins University Information Security Institute

2006 - 2010

Director and Principal Investigator (PI), NSF ACCURATE Center

1995 - 1999

Adjunct Professor, New York University

Summer, 1999

Visiting Professor, École Normale Supérieure, Paris, France

1988 - 1993

Teaching Assistant, University of Michigan

Doctoral Committees

Doctoral Thesis Advisor: David Inyangson, JHU

Doctoral Thesis Advisor: Logan Kostick, JHU

Doctoral Thesis Advisor: Atheer Almogbil, JHU (May, 2024)

Doctoral Thesis Advisor: Tushar Jois, JHU (May, 2023)

Doctoral Thesis Advisor: Random Gwinn, JHU (May, 2022)

Doctoral Thesis Advisor: Karl Siil, JHU (May, 2022)

Doctoral Thesis Advisor: James Cervini, JHU (May, 2022)

Doctoral Thesis Advisor: Jeff Chavis, JHU (May, 2021)

Doctoral Thesis Advisor: Gabe Kaptchuk, JHU (May, 2020)

Dissertation Committee: Thomas Tantillo, JHU (September, 2018)

Doctoral Thesis Advisor: Paul Martin, JHU (February, 2016)

Doctoral Thesis Advisor: Michael Rushanan, JHU (May, 2016)

Doctoral Thesis Advisor: Ayo Akinyele, JHU (December, 2013)

Doctoral Thesis Advisor: Matthew Pagano, JHU (August, 2013)

Doctoral Thesis Advisor: Ryan Gardner, JHU (August, 2009)

Doctoral Thesis Advisor: Sam Small, JHU (May, 2009)

Doctoral Thesis Advisor: Sujata Doshi, JHU (May, 2009)

Doctoral Thesis Advisor: Joshua Mason, JHU (June, 2009).

Dissertation Committee: J. Alex Halderman, Princeton University (May, 2009).

Dissertation Committee: Sophie Qiu (May, 2007).

Doctoral Thesis Advisor: Adam Stubblefield (April, 2005).

Dissertation Committee: Kevin FU, MIT (February, 2005).

Dissertation Committee: Robert Fischer, Harvard University (June, 2003).

Dissertation Committee: Marc Waldman, New York University, (April, 2003).

Dissertation Committee: Patrick McDaniel, U. of Michigan (September, 2001).

Doctoral Thesis Advisor: Fabian Monrose, New York University (April, 1999).

Dissertation Committee: Mike Just, Carleton University (November, 1998).

Dissertation Committee: Trent Jaeger, University of Michigan (October, 1996).

Industry Experience

2011 - present

Harbor Labs, Founder & Chief Scientist

2005 - 2011

Independent Security Evaluators, Founder & President

1997 - 2002

AT&T Labs -- Research, Secure Systems Research Department

1994 - 1996

Bellcore, Cryptography and Network Security Research Group

Summer, 1990

Great Lakes Software Co., Programmer, Howell, MI

Summer, 1989

IBM, Programmer, Meyers Corners Lab, Poughkeepsie, NY

Books

- Aviel D. Rubin, *Brave New Ballot*, Random House, (September, 2006).
- William R. Cheswick, Steven M. Bellovin and Aviel D. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker (2e)*, Addison Wesley Publishing Company, Inc., (February, 2003).
- **Chapter 4**, *Communications Policy and Information Technology: Promises, Problems, Prospects*, MIT Press, Lorrie Faith Cranor and Shane Mitchell Greenstein, eds., (2002).
- Aviel D. Rubin, *Whitehat Security Arsenal*, Addison Wesley Publishing Company, Inc., (June, 2001).
- **Chapter 8**, Publius and **Chapter 14**, Trust in Distributed Systems, Marc Waldman, Lorrie Faith Cranor, and Aviel D. Rubin, *PeertoPeer*, O'Reilly & Associates, Inc., (February, 2001).
- Aviel D. Rubin, Daniel Geer, Marcus J. Ranum, *Web Security Sourcebook*, John Wiley & Sons, Inc , (June, 1997).
- **Ph.D. dissertation**: *Nonmonotonic Cryptographic Protocols*, University of Michigan, Ann Arbor (April, 1994).

Refereed Journal Publications

- David Kotz, Kevin Fu, Carl Gunter, Avi Rubin, *Security for Mobile and Cloud Frontiers in Healthcare*, Communications of the ACM (July, 2015).
- Ayo Akinyele, Christina Garman, Matthew D. Green, Ian Miers, Matthew Pagano, Aviel D. Rubin, Michael Rushanan, *Charm: A Framework for Rapidly Prototyping Cryptosystems*, Journal of Cryptographic Engineering (JCEN), (January, 2013).
- Ryan Gardner, Sujata Garera, and Aviel D. Rubin, *Detecting Code Alteration by Creating a Temporary Memory Bottleneck*, IEEE Transactions on Information Forensics and Security: Special Issue on Electronic Voting, (December, 2009).
- Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, Avi Rubin, *Anonymity in Wireless Broadcast Networks*, International Journal of Network Security (IJNS), (January, 2008).
- Stephen Bono, Aviel Rubin, Adam Stubblefield, and Matthew Green, *Security Through Legality*, Communications of the ACM (June, 2006).
- Adam Stubblefield, Dan S. Wallach, and Aviel D. Rubin, *Managing the Performance Impact of Web Security*, Electronic Commerce Research Journal, February, 2005.
- David Jefferson, Aviel D. Rubin, Barbara Simons, David Wagner, *Analyzing Internet Voting Security*, Communications of the ACM (October, 2004).
- Simon Byers, Aviel D. Rubin, and David Kormann, *Defending Against an Internet-based Attack on the Physical World*, ACM Transactions on Internet Technology (TOIT), August, 2004.
- Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, *A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)* ACM Transactions on Information and System Security, May, 2004.

- Aviel D. Rubin, *Security Considerations for Remote Electronic Voting*, Communications of the ACM (December, 2002).
- Marc Waldman, Aviel D. Rubin, and Lorrie F. Cranor, *The Architecture of Robust Publishing Systems*, ACM Transactions on Internet Technology (TOIT), (November, 2001).
- David P. Kormann and Aviel D. Rubin, *Risks of the Passport Single-Signon Protocol*, Computer Networks, (July, 2000).
- Christian Gilmore, David P. Kormann, and Aviel D. Rubin, *Secure Remote Access to an Internal Web Server*, IEEE Network, (November, 1999).
- Fabian Monroe and Aviel D. Rubin, *Keystroke Dynamics as a Biometric for Authentication*, Future Generation Computer Systems, (March, 2000).
- Michael K. Reiter and Aviel D. Rubin, *Anonymity Loves Company: Anonymous Web Transactions with Crowds*, Communications of the ACM (February, 1999).
- Aviel D. Rubin and Daniel E. Geer, Jr., *Mobile Code Security*, IEEE Internet Computing (November/December, 1998).
- Aviel D. Rubin and Daniel E. Geer, Jr., *A Survey of Web Security*, IEEE Computer, (September, 1998).
- Michael K. Reiter and Aviel D. Rubin, *Crowds: Anonymity for Web Transactions*, ACM Transactions on Information and System Security, (June, 1998).
- Aviel D. Rubin, *An Experience Teaching a Graduate Course in Cryptography*, Cryptologia (April, 1997).
- Aviel D. Rubin, *Extending NCP for public Key Protocols*, Mobile Networks and Applications (ACM/Balzer), 2(3) (April, 1997).
- Aviel D. Rubin, *Independent One-Time Passwords*, USENIX Journal of Computer Systems (February, 1996).
- Aviel D. Rubin, *Secure Distribution of Documents in a Hostile Environment*, Computer Communications (June, 1995).

Refereed Conference Publications

- Tushar Jois, Gabrielle Beck, Sofia Belikovetsky, Joseph Carrigan, Alishah Chator, Logan Kostick, Maximilian Zinkus, Gabriel Kaptchuk, Aviel D. Rubin, *SocloTy: Practical Cryptography in Smart Home Contexts*, Privacy Enhancing Technologies Symposium 2024 (PETS '24), (July, 2024).
- Atheer Almogbil , Momo Steele , Sofia Belikovetsky , Adil Inam, Olivia Wu, Aviel Rubin, Adam Bates, *Using Behavior Monitoring to Identify Privacy Concerns in Smarthome Environments*, NDSS Workshop on Security and Privacy in Standardized IoT (SDIoTSec), (February, 2024).
- Samra Kasim, Nawal Valliani, Nelson Ka Ki Wong, Shahin Samadi, Lanier Watkins and Aviel Rubin, *Explainable Autonomic Cybersecurity for Industrial Control Systems*, IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), (March, 2023).
- Valeti Manoj, Shao Wenda, Niu Sihan, Christopher Rouff, Lanier Watkins, Aviel Rubin, *Cybersecurity as a Tic-Tac-Toe Game Using Autonomous Forwards (Attacking) And Backwards (Defending) Penetration Testing in a Cyber Adversarial Artificial Intelligence System*, IEEE International Conference of Computer Science and Information Technology (ICOSNIKOM),(October, 2022).

- James Cervini & Aviel D. Rubin, *Don't Drink the Cyber: Extrapolating the Possibilities of Oldsmar's Water Treatment Cyberattack*, ICCWS 17th International Conference on Cyber Warfare and Security, (July, 2022).
- Gabriel Kaptchuk, Tushar Jois, Matthew Green, Aviel Rubin, *Make Steganography Great Again — Before It's Too Late*, Real World Crypto 2022, (April, 2022).
- James Cervini, Daniel Muller, Alexander Beall, Joseph Maurio, Aviel Rubin & Lanier Watkins, *A Backfit Approach for Trusted Virtualization-Based Programmable Logic Controller Resilience*, Sixteenth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, (March, 2022).
- Hedin Beattie, Lanier Watkins, William H. Robinson, Aviel Rubin, Shari Watkins, *Measuring and Mitigating Bias in AI-Chatbots*, 2022 IEEE International Conference on Assured Autonomy (ICAA'22), (March, 2022).
- Random Gwinn, Mark Matties, Aviel D. Rubin, *Wavelet Selection and Employment for Side-Channel Disassembly*, IEEE International Conference on Physical Assurance and Inspection of Electronics (PAINE), (December, 2021).
- Karl A Siil, Aviel D. Rubin, Matthew C. Elder, Anton T Dahbura, Matthew Green, Lanier Watkins, *Cost-Effective Mission Assurance Engineering Through Simulation*, The 2021 International Conference on Internet of Things and Intelligence Systems (IoTIS'21), (November, 2021).
- Gabriel Kaptchuk, Tushar Jois, Matthew Green, Aviel Rubin, *Meteor: Cryptographically Secure Steganography for Realistic Distributions*, 28th ACM Conference on Computer and Communications Security (CCS '21), (November, 2021).
- James Schaffter, Aviel Rubin and Lanier Watkins, *A Containerization-Based Backfit Approach for Industrial Control System Resiliency*, SafeThings '21 Workshop, (May, 2021).
- Tushar Jois, Claudia Moncaliano, Khir Henderson, Aviel D. Rubin, *WDPKR: Wireless Device Profiling Kit and Reconnaissance*, 2021 Hot Topics in the Science of Security (HotSoS) Symposium (April, 2021).
- Lanier Watkins, ChangHao Cho, John Hurley, Aviel D. Rubin, *Collaborative Global Impact Cloud Computing Risk Assessment Framework*, International IoT, Electronics and Mechatronics Conference (IEMTRONICS '21), (April, 2021).
- Jeffrey S. Chavis, Malcom Doster, Michelle Feng, Syeda Zeeshan, Samantha Fu, Elizabeth Aguirre, Antonio Davila, Kofi Nyarko, Aaron Kunz, Tracy Herriotts, Daniel Syed, Lanier Watkins, Anna Buczak, Aviel Rubin, *A Voice Assistant for IoT Cybersecurity*, Integrated STEM Education Conference (ISEC '21), (March, 2021).
- Lanier Watkins, Danzel Hamilton, Kevin Kornegay, Aviel Rubin, *Triaging Autonomous Drone Faults by Simultaneously Assuring Autonomy and Security in Autonomous Drones*, 55th Annual Conference on Information Sciences and Systems (CISS '21), (March, 2021).
- Lanier Watkins, James Ballard, Kevin Hamilton, William H. Robinson, Aviel Rubin, Cleon Davis, *Bio-Inspired, Host-based Firewall* (Refereed WIP paper), 23rd IEEE International Conference on Computational Science and Engineering (CSE), (December, 2020).
- Lanier Watkins, Yue Yu, Sifan Li, William H. Robinson, Aviel D. Rubin, *Using Deep Learning to Identify Security Risks of Personal Mobile Devices in Enterprise Networks*, The 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), (October, 2020).

- Lanier Watkins, Kevin D. Fairbanks, Chengyu Li, Mengdi Yang, William H. Robinson, Aviel D. Rubin, *A Black Box Approach to Inferring Characterizing, and Breaking Native Device Tracking Autonomy*, The 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), (October, 2020).
- Karl Siil, Aviel Rubin, Matthew Elder, Anton Dahbura, Matthew Green, Lanier Watkins, *Mission Assurance for Autonomous Undersea Vehicles*, IEEE Workshop on Assured Autonomous Systems (WAAS), (May, 2020).
- Jeffrey Chavis, Aaron Kunz, Lanier Watkins, Anna Buczak, Aviel Rubin, *A Capability for Autonomous IoT System Security: Pushing IoT Assurance to the Edge*, IEEE Workshop on Assured Autonomous Systems (WAAS), (May, 2020).
- Lanier Watkins, Shane Sartalamacchia, Richard Bradt, Karan Dhareshwar, Harsimar Bagga, William H. Robinson, Aviel Rubin, *Defending Against Consumer Drone Privacy Attacks: A Blueprint For A Counter Autonomous Drone Tool*, ISOC Workshop on Decentralized IoT Systems and Security (DISS 2020), (February, 2020).
- Adrian Cartagena, Gerald Rimmer, Thomas Van Dalsen, Lanier Watkins, William H. Robinson, Aviel D. Rubin, *Privacy Violating Opensource Intelligence Threat Evaluation Framework: A Security Assessment Framework for Critical Infrastructure Owners*, 10th Annual Computing and Communications Workshop and Conference (IEEE CCWC 2020), (January, 2020).
- Jeffrey Chavis, Lanier Watkins, Anna Buczak, Aviel D. Rubin, *Connected Home Automated Security Monitor (CHASM): Protecting IoT Through Application of Machine Learning*, 10th Annual Computing and Communications Workshop and Conference (IEEE CCWC 2020), (January, 2020).
- Lanier Watkins, Shreya Aggarwal, Omotola Akeredolu, William H. Robinson and Aviel D. Rubin, *Tattle Tail Security: An Intrusion Detection System for Medical Body Area Networks*, Workshop on Decentralized IoT Systems and Security (DISS '19), (February, 2019).
- Lanier Watkins, Juan Ramon, Gaetano Snow, Jessica Vallejo, William H. Robinson, Aviel D. Rubin, Joshua Ciocco, Felix Jedrzejewski, Jinglun Liu, Chengyu Li, *Exploiting Multi-Vendor Vulnerabilities as BackDoors to Counter the Threat of Rogue Small Unmanned Aerial Systems*, ACM Workshop on Mobile IoT Sensing, Security, and Privacy (Mobile IoT SSP '18), (June, 2018).
- Paul D. Martin, David Russel, Malek Ben Salem, Stephen Checkoway, Aviel D. Rubin, *Sentinel: Secure Mode Profiling and Enforcement for Embedded Systems*, Proc. ACM/IEEE International Conference on Internet-of-Things Design and Implementation, (April, 2018).
- Gabriel Kaptchuk, Matthew D. Green and Aviel D. Rubin, *Outsourcing Medical Dataset Analysis: A Possible Solution*, Financial Cryptography Conference, (April, 2017).
- Michael Rushanan, David Russell and Aviel D. Rubin, *Mallory-Worker: Stealthy Computation and Covert Channels using Web Workers*, Proceedings of the 12th International Workshop on Security and Trust Management, (September, 2016).
- Paul Martin, Michael Rushanan, Thomas Tantillo, Christoph Lehmann and Aviel Rubin, *Applications of Secure Location Sensing in Healthcare*, Proceedings of the 7th ACM Conference on Bioinformatics, Computational Biology, and Health Informatics, (October, 2016).

- Gabriel Kaptchuk and Aviel D. Rubin, *A Practical Implementation of a Multi-Device Split Application for Protecting Online Poker*, Proceedings of the 15th Annual Security Conference, (March, 2016).
- Aviel D. Rubin, *Taking Two-Factor to the Next Level: Protecting Online Poker, Banking, Healthcare and Other Applications*, Proceedings of the 2014 Annual Computer Security Applications Conference, Invited Keynote Essay, (December, 2014).
- Michael Rushanan, Aviel D. Rubin, Denis Foo Kune, Colleen M. Swanson, *Security and Privacy in Implantable Medical Devices and Body Area Networks*, IEEE Symposium on Security and Privacy-SoK Track (May, 2014).
- Christina Garman, Matthew Green, Ian Miers, Aviel D. Rubin, *Rational Zero: Economic Security for Zerocoin with Everlasting Anonymity*, 1st Workshop on Bitcoin Research (March, 2014).
- Paul Martin, Aviel Rubin and Rafae Bhatti, *Enforcing Minimum Necessary Access in Healthcare Through Integrated Audit and Access Control*, Health Informatics Symposium at the ACM Conference on Bioinformatics, Computational Biology, and Biomedical Informatics, (September, 2013).
- Ian M. Miers, Christina Garman, Matthew D. Green, Aviel D. Rubin, *Zerocoin: Anonymous Distributed e-Cash from Bitcoin*, Proc. IEEE Symposium on Security and Privacy (May, 2013).
- Ian M. Miers, Matthew D. Green, Christoph U. Lehmann, Aviel D. Rubin, *Vis-à-Vis Cryptography: Private and Trustworthy In-Person Certifications*, In Proceedings of the 3rd USENIX/HealthSec Workshop, (August, 2012).
- Joseph A. Akinyele, Matthew W. Pagano, Matthew D. Green, Christoph U. Lehmann, Zachary N. J. Peterson and Aviel D. Rubin, *Securing Electronic Medical Records Using Attribute-Based Encryption On Mobile Devices*, ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices, (October, 2011).
- Matthew D. Green, Aviel D. Rubin, *A Research Roadmap for Healthcare IT Security inspired by the PCAST Health Information Technology Report 4-page Extended Abstract*, In Proceedings of the 2nd USENIX/HealthSec Workshop, (August, 2011).
- Ryan Gardner, Sujata Garera, Aviel D. Rubin, *Designing for Audit: A Voting Machine with a Tiny TCB*, Financial Cryptography Conference, (January, 2010).
- Ryan Gardner, Sujata Garera, Matthew W. Pagano, Matthew D. Green, Aviel D. Rubin, *Securing Medical Records on Smart Phones*, Workshop on Security and Privacy in Medical and Home-Care Systems, (November, 2009).
- Ryan Gardner, Sujata Garera, Aviel D. Rubin, *Coercion Resistant End-to-end Voting*, Financial Cryptography Conference, (February, 2009).
- Ryan Gardner, Sujata Garera, Anand Rajan, Carols Rozas, Aviel D. Rubin, Manoj Sastry, *Protecting Patient Records from Unwarranted Access*, Future of Trust in Computing, (July, 2008).
- Sujata Garera, Niels Provos, Monica Chew and Aviel D. Rubin, *A Framework for Detection and Measurement of Phishing Attacks*, 5th ACM Workshop on Recurring Malcode (WORM '07), (November, 2007).
- Sujata Garera and Aviel D. Rubin, *An Independent Audit Framework for Software Dependent Voting Systems*, 14th ACM Conference on Computer and Communications Security, (November, 2007).

- Ryan Gardner, Sujata Garera, and Aviel D. Rubin, *On the Difficulty of Validating Voting Machine Software with Software*, In Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07), (August, 2007).
- Sujata Doshi, Fabian Monrose, and Aviel D. Rubin, *Efficient Memory Bound Puzzles using Pattern Databases*, 4th International Conference on Applied Cryptography and Network Security (ACNS'06), (June, 2006).
- Sophie Qiu, Patrick McDaniel, Fabian Monrose, and Aviel Rubin, *Characterizing Address Use Structure and Stability of Origin Advertisement in Interdomain Routing*, 11th IEEE Symposium on Computers and Communications, (June 2006).
- Zachary Peterson, Randal Burns, Joseph Herring, Adam Stubblefield, and Aviel D. Rubin, *Secure Deletion for a Versioning Filesystem*, Proc. USENIX Conference on File and Storage Technologies (FAST '05), (December, 2005).
- Stephen C. Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel D. Rubin, Michael Szydlo, *Security Analysis of a Cryptographically-Enabled RFID Device*, 14th USENIX Security Symposium, (August, 2005).
- Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, *Analysis of an Electronic Voting System*, Proc. IEEE Symposium on Security and Privacy (May, 2004).
- Nathanael Paul, David Evans, Aviel D. Rubin and Dan Wallach, *Authentication for Remote Voting*, ACM Workshop on Human-Computer Interaction and Security Systems (April, 2003).
- Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, and Aviel Rubin, *Protocols for Anonymity in Wireless Networks*, Proc. 11th International Workshop on Security Protocols (April, 2003).
- Geoffrey Goodell, William Aiello, Timothy Griffin, John Ioannidis, Patrick McDaniel, Aviel Rubin, *Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing*, Proc. ISOC Symposium on Network and Distributed System Security (February, 2003).
- Simon Byers, Aviel D. Rubin, David Kormann, *Defending Against an Internet-based Attack on the Physical World*, ACM Workshop on Privacy in the Electronic Society (November, 2002).
- Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*, Proc. ISOC Symposium on Network and Distributed System Security (February, 2002).
- Aviel D. Rubin, *Security Considerations for Remote Electronic Voting*, 29th Research Conference on Communication, Information and Internet Policy (TPRC2001), (October, 2001).
- Aviel D. Rubin and Rebecca N. Wright, *Offline generation of limited-use credit card numbers*, Financial Cryptography Conference, (February, 2001).
- Marc Waldman, Aviel D. Rubin, and Lorrie F. Cranor, *Publius, A robust, tamper-evident and censorship-resistant web publishing system*, 9th USENIX Security Symposium, (August, 2000).
- David P. Kormann and Aviel D. Rubin, *Risks of the Passport Single Sign-on Protocol*, 9th International World Wide Web Conference, (May, 2000).
- Patrick McDaniel and Aviel D. Rubin, *A Response to "Can we Eliminate Certificate Revocation Lists?"*, Financial Cryptography Conference, (February, 2000).

- William A. Aiello, Aviel D. Rubin, and Martin J. Strauss, *Using smartcards to secure a personalized gambling device*, 6th ACM Conference on Computer and Communications Security, (November, 1999).
- Ian Jermyn, Alain Mayer, Fabian Monroe, Michael K. Reiter, and Aviel D. Rubin, *The Design and Analysis of Graphical Passwords*, 8th USENIX Security Symposium, (August, 1999).
- Christian Gilmore, David Kormann, and Aviel D. Rubin, *Secure Remote Access to an Internal Web Server*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1999).
- Fabian Monroe, Peter Wykoff, and Aviel D. Rubin, *Distributed Execution with Remote Audit*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1999).
- Dahlia Malkhi, Michael K. Reiter and Aviel D. Rubin, *Secure Execution of Java Applets using a Remote Playground*, Proc. IEEE Symposium on Security and Privacy (May, 1998).
- Aviel D. Rubin, Dan Boneh, and Kevin Fu, *Revocation of Unread Email in an Untrusted Network*, Second Australasian Conference on Information Security and Privacy (July, 1997).
- Fabian Monroe and Aviel D. Rubin, *Authentication via Keystroke Dynamics*, 4th ACM Conference on Computer and Communications Security (April, 1997).
- David M. Martin, Siviramakrishnan Rajagopalan, and Aviel D. Rubin, *Blocking Java Applets at the Firewall*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1997).
- Trent Jaeger, Aviel D. Rubin and Atul Prakash, *A System Architecture for Flexible Control of Downloaded Executable Content*, 5th International Workshop on Object-Orientation in Operating Systems (October, 1996).
- Trent Jaeger, Aviel D. Rubin and Atul Prakash, *Building Systems that Flexibly Control Downloaded Executable Content*, Proc. 6th USENIX Security Symposium (July, 1996).
- Victor Shoup and Aviel D. Rubin, *Session Key Distribution Using Smart Cards*, Proc. of Eurocrypt '96 (May, 1996).
- Trent Jaeger & Aviel D. Rubin, *Preserving Integrity in Remote File Location and Retrieval*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1996).
- Aviel D. Rubin, *Extending NCP for Public Key Protocols*, Proc. IEEE 4th International Conference on Computer Communications and Networks (September, 1995).
- Aviel D. Rubin, *PseudoRandom Functions for OneTime Passwords*, Proc. 5th USENIX UNIX Security Symposium (June, 1995).
- Aviel D. Rubin, *Trusted Distribution of Software Over the Internet*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1995).
- Aviel D. Rubin & Peter Honeyman, *Nonmonotonic Cryptographic Protocols*, Proc. IEEE Computer Security Foundations Workshop VII (June, 1994).
- Aviel D. Rubin & Peter Honeyman, *Long Running Jobs in an Authenticated Environment*, Proc. 4th USENIX UNIX Security Symposium (October, 1993).

Patents

- Aviel D. Rubin, "Broadband Certified Mail", **US Patent Numbers 6,990,581**, (January 24, 2006) and 9,876,769, (January 23, 2018).

- Aviel D. Rubin, Utilization of multiple devices to secure online transactions, **US Patent Number 9,064,376**, (June 23, 2015).
- Steven M. Bellovin, Thomas J. Killian, Bruce LaRose, Aviel D. Rubin, Norman L. Schryer, Method and apparatus for connection to virtual private networks for secure transactions, **US Patent Numbers 8,239,531**, (August 7, 2012) and **8,676,916** (March 18, 2014).
- Christian A. Gilmore, David P. Kormann, and Aviel D. Rubin, Method and apparatus for secure remote access to an internal web server, **US Patent Number 7,334,126**, (February 19, 2008).
- Aviel D. Rubin, "Method for secure remote backup", **US Patent Number 7,222,233**, (May 22, 2007).
- Frederick Douglass, Michael Rabinovich, Aviel D. Rubin, and Oliver Spatscheck, "Method for content distribution in a network supporting a security protocol", **US Patent Number 7,149,803**, (December 12, 2006).
- William A. Aiello, Steven M. Bellovin, Charles Robert Kalmanek, Jr., William T. Marshall, and Aviel D. Rubin, "Method and apparatus for enhanced security in a broadband telephony network", **US Patent Number 7,035,410**, (April 25, 2006).
- William A. Aiello, Aviel D. Rubin, and Martin J. Strauss, "Using smartcards to enable probabilistic transaction on an untrusted device", **US Patent Number 6,496,808**, (December 17, 2002).
- Aviel D. Rubin and Victor J. Shoup, "Session Key Distribution Using Smart Cards", **US Patent Number 5,809,140**, (September 15, 1998).
- Aviel D. Rubin, "Method for the Secure Distribution of Electronic Files in a Distributed Environment", **US Patent Number 5,638,446**, (June 10, 1997).

Professional Activities

Board of Directors

Director, Maryland Israel Development Center (MIDC), (2013-2018).

Director, USENIX Organization, elected by popular vote (2000-2004).

Editorial and Committees

Chair: IEEE Security & Privacy Symposium Test of Time Awards Committee for 2008-2010 Conferences, May, 2020.

Associate Editor: IEEE Transactions on Information Forensics and Security (2009 - 2011).

Associate Editor: Communications of the ACM (CACM), 2009 - 2017.

Guest Co-Editor: IEEE Transactions on Information Forensics and Security: Special Issue on Electronic Voting, December 1, 2009.

Guest Co-Editor: IEEE Security & Privacy Magazine, Special Issue on Electronic Voting, October/November, 2007.

Associate Editor: IEEE Transactions on Software Engineering (2005-2006). Editorial and

Advisory Board: International Journal of Information and Computer Security (IJICS) (2004 - 2006).

Guest Co-Editor: IEEE Computer Networks, Special Issue on Web Security, January, 2005.

Editorial Board: Journal of Privacy Technology (2004-2006).

Guest Co-Editor: IEEE Security & Privacy Magazine, Special Issue on Electronic Voting Security, January/February, 2004.

Member: Security Peer Review Group (SPRG) of the Federal Voting Assistance Program's (FVAP) Secure Electronic Registration and Voting Experiment (SERVE) Project, 2003 - 2004.

Member: DARPA Information Science And Technology Study Group (2003 - 2006).

Associate Editor: IEEE Security & Privacy Magazine (2003 - 2011).

Guest Editor: Communications of the ACM, Special Issue on Wireless Networking Security, May, 2003.

Associate Editor: ACM Transactions on Internet Technology (2002-2005).

Executive Committee Member: DIMACS Workshop Series with Special Focus on Network Security (2002 - 2004).

Advisory Board Member: Information Security and Cryptography Book Series, Springer, 2001- 2006.

Member: Steering Group, ISOC Symposium on Network and Distributed System Security, 2001 - 2004.

Member: Government Infosec Science and Technology Study Group on malicious code, 1999 - 2000.

Member: AT&T Internet Intellectual Property Review Team, 1999 - 2001. Associate Editor: Electronic Commerce Research Journal, Baltzer Science Publishers, 1999 - 2002.

CoEditor: Electronic Newsletter of the IEEE Technical Committee on Security & Privacy, with Paul Syverson, 1998.

Editorial Board: Bellcore Security Update Newsletter, 1995 - 1996.

Conference Committees

- **Program Committee member:** NDSS Workshop: Innovative Secure IT Technologies Against COVID19, San Diego, CA, February, 2020.
- **Program Committee member:** Financial Cryptography '15 Barbados, February, 2015.
- **Program Committee member:** USENIX HealthTech Workshop on Health Information Technologies (HealthTech '15), August 11, 2015.
- **Program Co-chair:** (w/Eugene Vasserman) USENIX HealthTech Workshop on Health Information Technologies (HealthTech '14), August 19, 2014.
- **Program committee member:** 2nd USENIX Workshop on Health Security & Privacy (HealthSec '11), August 9, 2011.
- **Program Co-chair:** (w/Kevin Fu & Yoshi Kohno), 1st USENIX Workshop on Health Security and Privacy (HealthSec '10), August 10, 2010.
- **Program Committee member:** First Security and Privacy in Medical and HomeCare Systems Workshop (SPIMACS), Chicago, IL, November 13, 2009.
- **Invited Talks Co-Coordinator:** 17th USENIX Security Symposium, San Jose, CA, July 28 August 1, 2008.
- **Program Co-chair:** (w/Patrick McDaniel): IEEE Symposium on Security and Privacy, Oakland, California, May 18-22, 2008.
- **Program Co-chair:** (w/Giovani Di Crescenzo): Financial Cryptography '06 Anguilla BWI, February, 2006.
- **Program Committee member:** IEEE Symposium on Security and Privacy, Oakland, California, May 9-12, 2004.
- **Program Committee member:** Financial Cryptography '04 Key West, Florida, February 9-12, 2004.

- **Program Committee member:** 2nd ACM SIGSAC Workshop on Privacy in the Electronic Society Washington D.C., October 30, 2003.
- **Program Committee member:** 10th ACM Conference on Computer and Communications Security, Washington D.C., October 27-30, 2003.
- **Program Committee member:** 8th European Symposium on Research in Computer Science (ESORICS), Norway, October 13-15, 2002.
- **Program Vice Chair:** Security and Privacy Track, The Twelfth International World Wide Web Conference, Budapest, Hungary, May 2004, 2003.
- **Program Committee member:** IEEE Symposium on Security and Privacy, Oakland, California, May 11-14, 2003.
- **Program Committee member:** Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, January 28, 2003.
- **Program Committee member:** 4th International Conference on Information and Communications Security (ICICS), Kent Ridge Digital Labs (KRD), Singapore December 9-12, 2002.
- **Program Committee member:** ACM SIGSAC Workshop on Privacy in the Electronic Society Washington D.C., November 21, 2002.
- **Program Committee member:** 9th ACM Conference on Computer and Communications Security, Washington D.C., November 17-21, 2002.
- **Program Committee member:** 5th International Conference on Electronic Commerce Research (ICECR5), Montreal, Canada, October 23-27, 2002.
- **Program Committee member:** 2nd Symposium on Requirements Engineering for Information Security (SREIS), Raleigh, North Carolina, Oct 14-15, 2002.
- **Program Committee member:** 7th European Symposium on Research in Computer Science (ESORICS), Zurich, Switzerland, October 14-16, 2002.
- **Program Committee member:** 11th USENIX Security Symposium, San Francisco, Ca, August 5-9, 2002.
- **Program Committee member:** International Workshop on Global and Peer-to-Peer Computing at IEEE International Symposium on Cluster Computing and the Grid (CCGrid'2002), Berlin, Germany, May 21-24, 2002.
- **Program Committee member:** 11th International World Wide Web Conference Honolulu, Hawaii, May 7-11, 2002.
- **Program Committee member:** 2nd Workshop on Privacy Enhancing Technologies San Francisco, CA, April 14-15, 2002.
- **Program Committee member:** The 1st International Workshop on Peer-to-Peer Systems (IPTPS'02) MIT Faculty Club, Cambridge, MA, March 7-8, 2002.
- **Program Committee member:** The 4th International Conference on Telecommunications and Electronic Commerce Dallas, TX, November, 2001. **Program Committee member:** 10th USENIX Security Symposium, Washington D.C., August 13-17, 2001.
- **Program Committee member:** Financial Cryptography '01 Grand Cayman, Cayman Islands, BVI, February, 2001.
- **Program Co-chair:** (w/Paul Van Oorschot): ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 7-9, 2001.
- **Program Committee member:** The 3rd International Conference on Telecommunications and Electronic Commerce Dallas, TX, November 16-19, 2000. **Program Committee member:** 9th USENIX Security Symposium, Denver, Colorado, August 14-17, 2000.

- **Program Committee member:** Workshop on Design Issues in Anonymity and Unobservability Berkeley, California, July 2526, 2000.
- **Program Committee member:** Performance and Architecture of Web Servers (PAWS), Santa Clara, CA, June 18, 2000.
- **Program Co-chair:** (w/Gene Tsudik): ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 24, 2000.
- **Program Committee member:** 1999 International Information Security Workshop (ISW'99), Kuala Lumpur, Malaysia, November 67, 1999.
- **Program Committee member:** 2nd Int'l. Conference on Telecommunications and Electronic Commerce, Nashville, TN, October 68, 1999.
- **Invited Talks coordinator:** 8th USENIX Security Symposium, Washington D.C., August, 1999.
- **Program Chair:** 24th USENIX Annual Technical Conference, Monterey, CA, June 711, 1999.
- **Program Committee member:** 8th International World Wide Web Conference , Toronto, Canada, May 1114, 1999.
- **Program Committee member:** 3rd USENIX workshop on Electronic Commerce , Boston, MA, August 31 September 3, 1998.
- **Program Committee member:** 5th ACM Conference on Computer and Communications Security, San Francisco, CA, November 35, 1998.
- **Program Chair:** 7th USENIX Security Symposium, San Antonio, TX, Jan. 2629, 1998.
- **Program Committee member:** 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, April 24, 1997.
- **Program Committee member:** 6th USENIX Security Symposium, San Jose, CA, July 2225, 1996.
- **Program Committee member:** ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 2223, 1996.

Panels

- **Panelist:** CyberTech Global Conference: The Post-COVID Cyber Challenges in the Health Sector, UAE-Dubai (April 6, 2021).
- **Panel Organizer and Moderator:** USENIX Security Conference: The 2020 Election: Remote Voting, Disinformation, and Audit (August 12, 2020).
- **Panelist:** Cardozo Society Associated panel: Cybersecurity and Privacy Law in the Digital Era, Baltimore, MD (February 19, 2020).
- **Panelist:** Washington Post panel: Hacking Health, Washington DC (June 14, 2016).
- **Panelist:** Financial Cryptography Conference, Security & Privacy, Barbados (February 24, 2016).
- **Panelist:** RSA Conference, Social Networks Security Panel, San Francisco, CA (April 21, 2015).
- **Panelist:** Expert Witness in Mock Trial: FTC Data Security, 63rd American Bar Association Section of Antitrust Law Spring Meeting Washington DC, (April 15, 2015).
- **Panelist:** Security in Electronic Medical Records Databases, Medicine 2.0 Workshop, Haifa, Israel, (April 7, 2011).
- **Panelist:** Security in the Cloud, Workshop on Cloud Security, Israeli Defense Ministry, Tel Aviv, Israel, (February 15, 2011).

- **Panelist:** Securing Information Technology in Healthcare (SITH), Security and Usability of Electronic Health Records, Dartmouth College, NH, (May 17, 2010).
- **Panelist:** First Security and Privacy in Medical and HomeCare Systems Workshop (SPIMACS), Authentication in iHealthcare, Chicago, IL, (November 13, 2009).
- **Panelist:** Computers, Freedom, and Privacy Conference, Internet Voting for Overseas Americans, Washington DC, (June 4, 2009).
- **Panelist:** Workshop on Electronic Voting, Electronic Voting: Future Aspirations, Tel Aviv, Israel (May 18, 2009).
- **Panelist:** RSA Conference, Exploiting Online Games, San Francisco, CA (April 23, 2009).
- **Panelist:** American Association for the Advancement of Science, Revisiting the U.S. Voting System: A Research Inventory, Technology, Usability, and Security panel, Washington DC, (November 27, 2006).
- **Panelist:** California Secretary of State's Voting System Testing Summit, Security Panel, Sacramento, CA, (November 2829, 2005).
- **Panelist:** NIST Symposium on Voting System Threats, Configuration and Usability Threats, Gaithersburg, MD, (October 7, 2005).
- **Panelist:** Conference of State Supreme Court Chief Justices, Voting Technologies, Charleston, SC (August 1, 2005).
- **Panelist:** Workshop on observation of automated elections, The Carter Center, Atlanta, GA (March 18, 2005).
- **Panelist:** The Carter Center Venezuela Virtual Panel, (November, 2004).
- **Panelist:** Workshop on Voting, Vote Capture and Vote Counting, Harvard Kennedy School of Government, The Technologies of Voting, Cambridge, MA (June 1, 2004).
- **Panelist:** Computer Science and Telecommunications Board of The National Academy of Science Workshop on Dependable Software Systems, Case Study: Electronic Voting Washington D.C. (April 20, 2004).
- **Panelist:** USENIX Security 2003, Electronic Voting, Washington D.C. (August 6, 2003).
- **Panelist:** Democracy Now, 2003, Voter-Verifiable Elections: How Do We Get There?, Washington D.C. (November 23, 2003).
- **Panelist:** USENIX Security 2003, Electronic Voting, Washington D.C. (August 6, 2003).
- **Panelist:** IEEE Infocom 2002, Securing Wireless and Mobile Networks, Is It Possible?, New York City (June 25, 2002).
- **Participant:** 2002 Security Visionary Roundtable: A Roadmap for a Safer Wireless World, Washington D.C., (May 5-7, 2002).
- **Panelist:** Computers Freedom and Privacy 2002, Who Goes There? Privacy in Identity and Location Services, San Francisco (April 18, 2002).
- **Panel moderator:** Conference on Democracy and the Internet in an Enlarging Europe Overview of On-Line Voting: Systems and Issues, New York, NY (March, 2001).
- **Panelist:** Financial Cryptography 2001, The Business of Electronic Voting, Grand Cayman (February, 2001).
- **Panelist:** National Science Foundation E-voting workshop, Washington, D.C., (October, 2000).
- **Panelist:** 5th ACM Conference on Computer and Communications Security, Anonymity on the Internet, San Francisco, CA, (November, 1998).
- **Panelist:** Open Systems Security and ISSA Annual Conference, Securing the Web, Orlando, FL (March, 1998).

- **Panel organizer and moderator:** Implementation Issues for Electronic Commerce: What Every Developer Should Know. ISOC Symposium on Network and Distributed System Security, (March, 1998).
- **Panel organizer and moderator:** Downloadable Executable Content Past, Present and Future. ISOC Symposium on Network and Distributed System Security (February, 1997).
- **Panelist:** DIMACS Workshop on Network Threats, Web/Java Security Issues, New Brunswick, NJ (December 5, 1996).

Testimony

Before Government Bodies

- United States House Committee on Administration, Full Committee Hearing, Exploring the Feasibility and Security of Technology to Conduct Remote Voting in the House, Live via WebEx, (July 17, 2020).
- Maryland House, Expert Testimony, Hearing on HB 888, Consumer Protection, Security Features for Connected Devices, Economic Matters Committee, Annapolis, MD, (February 26, 2020).
- Maryland Senate, Expert Testimony, Hearing on SB 443 Security Features for Connected Devices, Finance Committee, Annapolis, MD, (February 19, 2020).
- Maryland Senate, Expert Testimony, Hearing on SB 553/HB 1276 Security Features for Connected Devices, Finance Committee, Annapolis, MD, (February 26, 2019). United States Pentagon, High Level Security Briefing on the Security of Embedded Devices (January 15, 2014).
- United States House Committee on Science, Space, and Technology, Full Committee Hearing Is My Data on Healthcare.gov Secure?, Washington, D.C., (November 19, 2013).
- United States House Committee on Oversight and Government Reform, hearing on electronic voting, Washington, D.C., (April 18, 2007).
- United States House Committee on Appropriations, hearing on ensuring the integrity of elections, Washington, D.C., (March 7, 2007).
- Maryland Senate Committee on Education, Health, and Environmental Affairs, Expert Testimony, Hearing on Senate Bill 392 for Voter Verified Records in Voting Systems, Annapolis, MD, (February 22, 2007).
- Maryland House Ways and Means Committee, Expert Testimony, Hearing on House Bill 18 for improving voting systems in Maryland, Annapolis, MD, (February 1, 2007).
- Maryland House Ways and Means Committee, Expert Testimony, Hearing on House Bill 244 requiring a voter verified paper record for voting machines in Maryland, Annapolis, MD, (February 1, 2006).
- United States Election Assistance Commission, Hearing on Voluntary Voting Systems Guidelines, Expert Testimony, Panel on Voter Verified Paper Audit Trail, Washington D.C. (June 30, 2005).
- Senate hearing: Voting in 2004: A Report to the Nation on America's Election Process, Expert Testimony, Absentee Ballot Panel, Dirksen Senate Office Building, Washington, DC (December 7, 2004).
- United States Election Assistance Commission, Technical Guidelines Development Committee, Technology Panel, Expert Testimony, Public Hearings on Computer

Security and Transparency, National Institute of Standards and Technology, Gaithersburg, MD, (September 20, 2004).

- United States House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Expert Testimony, Hearing on Electronic Voting, Washington, D.C. (July 20, 2004).
- United States House Committee on House Administration, Expert Testimony, Hearing on Security of Electronic Voting, Washington, D.C. (July 7, 2004).
- United States Federal Trade Commission, Written Expert Testimony, on a proposed Do Not Email Repository, (May 10, 2004).
- United States Election Assistance Commission, Expert Testimony, Hearing on Electronic Voting Security, Technology Panel, Washington D.C. (May 5, 2004).

As an Expert in Litigation

- Epic Games, Inc & Anor vs. **Apple Inc & Anor.**, Case # NSD 1236 of 2020, Gibson Dunn, Federal Court of Australia, District of New South Wales. (App Store Security & Privacy)
 - Expert Testimony at Trial, Melbourne, Australia (May 29, 2024).
- **Proxense, LLC**, vs. Google., Case # 6:23-cv-00320-ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent claim construction)
 - Expert Testimony at deposition, Key West, FL (December 18, 2023).
- **Softex LLC** vs Absolute Software Corporation, Dell Technologies Inc, and HP Inc, Case # 1:22-cv-01309-DAE; McKool Smith, United States District Court, Western District of Texas. (Patent Claim Construction)
 - Expert Testimony at deposition, Key West, FL (November 27, 2023).
- **Milliman, Inc** and Vigilytics LLC, vs. Gradient A.I. Corp., Case # 1:21-cv-10865-NMG; K&L Gates, United States District Court, District of Massachusetts. (Patent Claim Construction, Patent Infringement, Patent Validity, Trade Secret)
 - Expert Testimony at deposition, Annapolis, MD (November 27, 2023).
 - Expert Testimony at deposition, Annapolis, MD (November 17, 2022).
- Microsoft Corporation vs. **Mediapointe, Inc**, Case # 2:22-cv-01009-MCS-MRW; Susman Godfrey, United States District Court, Central District of California. (Patent Infringement & Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (September 29, 2023).
- Akamai Technologies, Inc vs. **Mediapointe, Inc**, Case # 2:22-cv-06233-MCS-AFM; Susman Godfrey, United States District Court, Central District of California. (Patent Infringement & Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (September 22, 2023).
- Lauri Valjakka vs. **Netflix Inc**, Case # 4:22-cv-01490-JST, Perkins Coie, United States District Court, Northern District of California. (patent Non-infringement and patent invalidity)
 - Expert Testimony at Deposition, Annapolis, MD (September 8, 2023).
- **TecSec Inc** vs. Oracle, Case # 1:10CV 115 LO-TCB; Hunton & Williams, United States District Court, Eastern District of Virginia. (Patent Infringement, Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (June 13, 2023).
 - Expert Testimony at deposition, Annapolis, MD (September 11, 2020).

- Global Eticket Exchange Ltd. vs. **TicketMaster LLC**, Case # 6:21-cv-00399-ADA, Fish & Richardson, United States District Court, Western District of Texas. (Patent Non-infringement and validity)
 - Expert Testimony at Trial, Waco, TX (May 3, 2023).
 - Expert Testimony at Deposition, Annapolis, MD (January 31, 2023).
 - Expert Testimony at Deposition, Annapolis, MD (January 16, 2023).
- **Fanduel, Inc** vs. Winview, Inc, IPR 2022-01306, ArentFox Schiff, US Patent Trial and Appeal Board. (Patent Invalidity)
 - Expert Testimony at deposition, Annapolis, MD (April 20, 2023).
- **Fanduel, Inc** vs. Winview, Inc, IPR 2022-01307, ArentFox Schiff, US Patent Trial and Appeal Board. (Patent Invalidity)
 - Expert Testimony at deposition, Annapolis, MD (April 19, 2023).
- **TecSec Inc** vs. Cisco, Case # 1:10-CV 115 LO-TCB; Hunton & Williams, United States District Court, Eastern District of Virginia. (Patent Infringement, Patent Validity)
 - Expert Testimony at deposition, Washington DC (April 12, 2023).
 - Expert Testimony at deposition, Annapolis, MD (September 14, 2020).
- **WSOU Investments, LLC**, vs. Cisco Systems Inc., Case # 6:21-cv-00128-ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent Infringement & Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (March 30, 2023).
 - Expert Testimony at deposition, Annapolis, MD (January 18 & 19, 2023).
- Finjan vs. **Palo Alto Networks**, Case # 4:14-CV-04908-PJH, Morrison and Foerster, United States District Court, Northern District of California.
 - Expert Testimony at Deposition, Annapolis, MD (March 17, 2022). (*Patent Non-infringement and invalidity*)
 - Expert Testimony at Deposition, Annapolis, MD (March 15, 2022). (*Patent Non-infringement and invalidity*)
 - Expert Testimony at Deposition, Pikesville, MD (August 16, 2021). (*Claim Construction*)
- Centripetal Networks, Inc. vs. **Keysight Technologies, Inc.**, Investigation No. 337-TA-1314-MJM, Reed Smith LLP, United States International Trade Commission (ITC). (Patent Non-infringement & Domestic Industry Technical Prong)
 - Expert Testimony at Trial, Washington DC (March 6, 2023).
 - Expert Testimony at Deposition, Las Vegas, NV (December 2, 2022).
- **Proxense, LLC**, vs. Samsung Electronics Co., Case # 6:21-cv-00210ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent Infringement & Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (January 12, 2023).
 - Expert Testimony at deposition, Annapolis, MD (September 30, 2022).
 - Expert Testimony at deposition, Annapolis, MD (September 29, 2022).
- **US Dominion, Inc.** vs. Fox News Network, Case # N21C-03-257-EMD, Susman Godfrey, United States District Court, District of Delaware. (Defamation)
 - Expert Testimony at deposition, Annapolis, MD (January 10, 2022).
- **Rimini Street, Inc.** vs. Oracle International Corporation, et. al., Case # 2:14-CV-01699 LRHCWH, Gibson Dunn, United States District Court, District of Nevada. (Software security)

- Expert Testimony at trial, Las Vegas, NV (December 9, 2022).
- Expert Testimony at deposition, Baltimore, MD (August 30, 2018).
- **IOEngine, LLC**, vs. Ingenico Inc., Case # 1:18-cv-826 WCB; Dechert LLP, United States District Court, District of Delaware. (Patent Infringement & Patent Validity)
 - Expert Testimony at trial, Wilmington, DE (July 12 & 14, 2022).
 - Expert Testimony at deposition, Annapolis, MD (January 28, 2022).
 - Expert Testimony at deposition, Bonita Springs, FL (January 19, 2022).
- **WSOU Investments, LLC**, vs. Microsoft Corporation, Case # 6:20-cv-00464-ADA; Susman Godfrey, United States District Court, Western District of Texas. (Patent Infringement and Patent Validity)
 - Expert Testimony at deposition, Annapolis, MD (May 15 & 16, 2022).
- **10Tales Inc.** vs. TikTok PTE. LTD., Case # 4:21-cv-3868-YGR; Cozen O'Connor, United States District Court, Northern District of California. (Patent Claim Construction)
 - Expert Testimony at deposition, Annapolis, MD (May 11, 2022).
- **IOEngine, LLC**, vs. PayPal Holdings, Inc., Case # 1:18-cv-452-WCB; Dechert LLP, United States District Court, District of Delaware. (Patent infringement)
 - Expert Testimony at deposition, Bonita Springs, FL (January 18, 2022).
 - Expert Testimony at deposition, Bonita Springs, FL (January 26, 2022).
- AGIS Software Development LLC vs. **Uber Technologies Inc.**, Case # 2:21-cv-00026-JRG-RSP, Gibson Dunn, United States District Court, Eastern District of Texas. (Non-infringement)
 - Expert Testimony at Deposition, Annapolis, MD (December 22, 2021).
- Sable Networks vs. **Splunk Inc.**, Case # 5:21-CV-00040-RWS, Morrison and Foerster, United States District Court, Eastern District of Texas. (Claim Construction)
 - Expert Testimony at Deposition, Annapolis, MD (December 13, 2021).
- Huawei Technologies Co. vs. **Verizon Communications Inc.**, Case # 6:20-CV-00090, Quinn Emanuel, United States District Court, Western District of Texas. (Patent Non-infringement and patent invalidity)
 - Expert Testimony at Deposition, Pikesville, MD (July 1, 2021).
- Epic Games, Inc. vs. **Apple Inc.**, Case # 4:20-cv-05640-YGR-TSH, Gibson Dunn, United States District Court, Northern District of California. (Sherman Act)
 - Expert Testimony at Trial, Oakland, CA (May 20-21, 2021).
 - Expert Testimony at Deposition, Pikesville, MD (March 26, 2021).
- Philips North America LLC ; Koninklijke Philips N.V. vs. **Summit Imaging Inc.**, Case # 2:19cv01745JLR, Seed IP, United States District Court, Western District of Washington at Seattle. (DMCA and Copyright)
 - Expert Testimony at deposition, Pikesville, MD (March 16, 2021).
- **California Physicians Service, Inc D/B/A Blue Shield of California** vs. Healthplan Services Inc, Case # 3:18-cv-3730 Latham & Watkins, United States District Court, Northern District of California. (Contract Dispute: Software Quality and Security)
 - Expert Testimony at Deposition, Pikesville, MD (March 9, 2021).
- Finjan vs. **Qualys Inc.**, Case # 4:18-cv-07229-YGR, Wilson Sonsini, United States District Court, Northern District of California. (patent invalidity and Non-infringement)
 - Expert Testimony at Deposition, Pikesville, MD (March 4, 2021).

- Finjan vs. **Sonicwall Inc.**, Case # 5:17-cv-04467-BLF-HRL, Duane Morris, United States District Court, Northern District of California. (patent invalidity and Non-infringement)
 - Expert Testimony at deposition, Pikesville, MD (October 30, 2020).
 - Expert Testimony at deposition, Pikesville, MD (October 29, 2020).
- **Blackberry Limited** vs. Facebook, Inc, Case #2:18-cv-01844 (KSx), Quinn Emanuel Urquhart & Sullivan, LLP, United States District Court, Central District of California. Expert Testimony at Deposition, Baltimore, MD (December 20, 2019). (patent infringement & patent validity)
- **Netfuel, Inc.** vs. Cisco Systems, Inc, Case # 5:18-cv-2352-EJD, Susman Godfrey, United States District Court, Northern District of California.
 - Expert Testimony at Deposition, Baltimore, MD (December 16 & 17, 2019). (patent infringement & patent validity)
 - Expert Testimony at Deposition, Baltimore, MD (June 11, 2019). (patent infringement)
 - Expert Testimony at Markman Hearing, San Jose, CA (February 28, 2019). (courtroom tutorial)
 - Expert Testimony at deposition, Baltimore, MD (December 20, 2018). (claim construction)
- **Symantec Corporation** vs. Zscaler, Inc., Case # 3:17-CV-04414-JST, Baker Botts, United States District Court, Northern District of California.
 - Expert Testimony at Deposition, Baltimore, MD (December 6, 2019). (patent infringement)
 - Expert Testimony at Deposition, Baltimore, MD (August 2, 2019). (Assignor Estoppel)
- Koninklijke Philips vs. **Microsoft Inc**, Case # 4:18-cv-01885-HSG, Perkins Coie, United States District Court, Northern District of California. (patent Non-infringement and patent invalidity)
 - Expert Testimony at Deposition, Baltimore, MD (July 17, 2019).
- **Cypress Lake Software, Inc.** vs. Samsung Electronics & Dell Inc, Case # 6:18-cv-030-JKD and 6:18cv0138JDK, Garteiser Honea, United States District Court, Eastern District of Texas. (patent infringement and patent validity)
 - Expert Testimony at Deposition, Baltimore, MD (July 1011, 2019).
- Finjan vs. **Juniper Networks**, Case # 3:17-cv-05659-WHA , Irell and Manella, United States District Court, Northern District of California.
 - Expert Testimony at deposition, Baltimore, MD (April 2, 2019). (patent Non-infringement)
 - Expert Testimony at deposition, San Francisco, CA (March 9, 2019). (patent Non-infringement)
 - Expert Testimony at trial, San Francisco, CA (December 13, 2018). (patent Non-infringement and invalidity)
 - Expert Testimony at deposition, Baltimore, MD (November 9, 2018). (patent Non-infringement and invalidity)
 - Expert Testimony at deposition, Baltimore, MD (July 6, 2018). (patent Non-infringement)

- Expert Testimony at deposition, Baltimore, MD (June 12, 2018). (patent Non-infringement)
- Grace et. al. vs. **Apple Inc.**, Case # 5:17-CV-00551LHK (NC), Durie Tangri, United States District Court, Northern District of California. (class action)
 - Expert Testimony at deposition, Towson, MD (September 26, 2018).
- Grace et. al. vs. **Apple Inc.**, Case # 5:17-CV-00551-LHK (NC), Kirkland & Ellis, United States District Court, Northern District of California. (class certification)
 - Expert Testimony at deposition, Pikesville, MD (July 3, 2018).
- **F5 Networks, Inc.** vs. Radware, LTD., IPR 2017-00124, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (January 24, 2018).
- **Amazon.com Inc., Hulu, LLC, and Netflix, Inc.** vs. Uniloc Luxembourg S.A., IPR 201700948, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (October 9, 2017).
- Phishme, Inc. vs. **Wombat Technologies, Inc.**, Case # 16403-LPS-CJB, K&L Gates, United States District Court, Delaware. (patent claim construction)
 - Expert Testimony at deposition, Washington DC, (October 5, 2017).
- Finjan vs. **Symantec Corporation.**, Case # 14-cv-02998-HSG, Quinn Emanuel, United States District Court, Northern District of California. (patent invalidity and Non-infringement)
 - Expert Testimony at deposition, Baltimore, MD (September 14-15, 2017).
- **Kudelski SA, Nagra USA, Inc., NagraVision SA, and OpenTV, Inc.** vs. Comcast Corporation, Case # 2:16-cv-1362-JRG, Covington, United States District Court, Eastern District of Texas. (patent claim construction).
 - Expert Testimony at deposition, Baltimore, MD (September 1, 2017).
- **F5 Networks, Inc.** vs. Radware, LTD., IPR 2017-00124, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (August 10, 2017).
- Intellectual Ventures vs. **JP Morgan Chase & Co.**, Case # 1:13-cv-03777, Kirkland & Ellis, United States District Court, Southern District of New York. (Patent Non-infringement).
 - Expert Testimony at deposition, Baltimore, MD (June 1, 2017).
- Nader AsghariKamrani and Kamran AsghariKamrani vs. **United Services Automobile Association.** Case # 2:15-CV-478, Fish & Richardson, United States District Court, Eastern District of Virginia. (Patent Written Description Support related to Inequitable Conduct).
 - Expert Testimony at trial, Norfolk, VA (April 21, 2017).
 - Expert Testimony at deposition, Baltimore, MD (March 21, 2017).
- **Sabre GBL Inc.** vs. HP Enterprise Services LLC. Case # 1310022761, JAMS Binding Arbitration Hearing, Dallas, TX (Contract dispute).
 - Expert Testimony at arbitration hearing, Dallas, TX (April 5, 2017).
- **Al Cioffi et. al.** vs. Google, Case # 2:13cv103JRGRSP, Vasquez, Benisek & Lindgren, United States District Court, Eastern District of Texas. (patent Infringement).
 - Expert Testimony at trial, Marshall, TX (February 7, 2016).
 - Expert Testimony at deposition, Baltimore, MD (September 26, 2016).

- **Palo Alto Networks** vs. Finjan, IPR 2015-01979, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (November 14, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2016-00151, Morrison & Foerster, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (August 19, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-01974, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (August 2, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-02001 & IPR 2016-00157, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (July 26 & 27, 2016).
- **Amazon.com, Inc** vs. Zitovault, LLC, IPR 2016-00021, Perkins Coie, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (July 22, 2016).
- **Palo Alto Networks** vs. Finjan, IPR 2015-01979, Cooley, US Patent Trial and Appeal Board. (patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (May 20, 2016).
- **Vir2us Inc. v. Invincea, Inc. and Invincea Labs, LLC**, Case # 2:15-cv-l62; Cooley, United States District Court, Eastern District of Virginia. (Patent Non-infringement and Invalidity)
 - Expert Testimony at deposition, Reston, VA (April 20, 2016).
- **TVIIM. v. McAfee Inc.**, Case # 3:13-cv-04545-VC; Wilmer Hale, United States District Court, District of N. California. (Patent Non-infringement and Invalidity)
 - Expert Testimony at trial, San Francisco, CA (July, 2015).
 - Expert Testimony at deposition, Baltimore, MD (February, 2015).
- **Intellectual Ventures vs. Symantec**, Case # 1:10-cv-01067-LPS; Latham & Watkins, United States District Court, District of Delaware. (Patent Invalidity)
 - Expert Testimony at trial, Wilmington, DE (February, 2015).
 - Expert Testimony at deposition, Baltimore, MD (May, 2013).
- **Rovi Solutions & Veracode** vs. Appthority, Case # 1210487-DPW; Goodwin Procter, United States District Court, District of Massachusetts. (Patent Infringement and Validity)
 - Expert Testimony at trial, Boston, MA (August 11, 2014).
 - Expert Testimony at deposition, Baltimore, MD (April 4, 2014).
- **Juniper** vs. Palo Alto Networks, Case # 1:11-CV-01258-SLR; Irell & Manella, United States District Court, District of Delaware. (Patent Infringement)
 - Expert Testimony at trial, Wilmington, DE (February, 2014).
 - Expert Testimony in court hearing, Wilmington, DE (November 14, 2013).
 - Expert Testimony at deposition, Baltimore, MD (June, 2013).
- **Prism Technologies. v. Adobe Systems Inc.**, Case # 8:10-cv-00220-LEST-DT; DLA Piper, United States District Court, District of Nebraska. (Patent Invalidity)
 - Expert Testimony at deposition, Baltimore, MD (August, 2012).
- **Finjan Inc. vs. McAfee, Inc.**, Case # 10593 (GSM), Kirkland & Ellis, United States District Court, District of Delaware. (Patent Non-infringement)
 - Expert Testimony at deposition, Washington, DC (June, 2012).

- Avaya Inc. vs. **Telecom Labs Inc., TeamTLI.com Corp., and Continuant Technologies**, Case # 3:06-cv-02490 (GEB); K&L Gates, United States District Court, District of New Jersey. (Contract Dispute)
 - Expert Testimony at deposition, Newark, NJ (August, 2011).
- **Lear Automotive** vs. Johnson Controls Inc (JCI), Case # 04-CV-73461; Flachsbart & Greenspoon, United States District Court, Eastern District of Michigan. (Patent Infringement and Validity)
 - Expert Testimony **at trial**, Detroit, MI (February, 2011).
 - Expert Testimony at deposition, Baltimore, MD (December, 2005).
- **TecSec Inc** vs. International Business Machines Corporation, Case # 1:10-CV-115-LMB/TCB; Hunton & Williams, United States District Court, Eastern District of Virginia. (Patent Infringement)
 - Expert Testimony at deposition, Newark, NJ (November, 2010).
- **Echostar Satellite Corporation** vs. NDS Group, Case # SA-CV-03950-DOC(JTL); T. Wade Welch & Associates, United States District Court, Central District of California. (Copyright and DMCA)
 - Expert Testimony **at trial**, Santa Ana, CA (April, 2008).
 - Expert Testimony at deposition, Santa Ana, CA (April, 2008).
 - Expert Testimony at deposition, Baltimore, MD (October, 2007).
- **Web.com Inc** vs. The Go Daddy Group Inc., Case # CV-0701552-PHX-MHM; Graves Law Office, United States District Court, Arizona. (Patent Infringement)
 - Expert Testimony at Markman hearing, Phoenix, Az (July, 2008).
 - Expert Testimony at deposition, Baltimore, MD (May, 2008).
- z4 Technologies vs. **Microsoft & Autodesk**, Case # 2:04-CV-00335-LED; Fish & Richardson, United States District Court, Eastern District of Texas. (Patent Non-Infringement and Invalidity)
 - Expert Testimony **at trial**, Tyler, TX, (April, 2006).
 - Expert Testimony at deposition, Washington DC (January, 2006).
- **Linda Schade** vs. Linda Lamone et. al., Trial on the Legality of Paperless Voting Machines in Maryland. (Adequacy of Voting Equipment)
 - Expert Testimony **at trial**, Annapolis, MD (August 25, 2004).

Awards

- 2020, **Best Paper Award**, in the category of Mobile & Wireless Computing, 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), October, 2020.
- 2020, **Best Paper Award**, in the category of Image Processing & Multimedia Technology, 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communications Conference (UEMCON), October, 2020.
- IEEE Computer Society Technical Committee on Security and Privacy, **Distinguished Service Award**, May, 2020.
- **Fulbright Scholar** in Israel at Tel Aviv University, academic year 2010-2011.
- 2009, **Google Research Award**, Securing Medical Records on Smartphones.
- Chosen as one of **54 favorite people, places and things in Jewish Baltimore**, Baltimore Jewish Times, February 22, 2008.

- 2007 **Award for Outstanding Research in Privacy Enhancing Technologies**, for Security Analysis of a Cryptographically Enabled RFID Device (with Stephen C. Bono, Matthew Green, Ari Juels, Adam Stubblefield, Michael Szydlo).
- 2005 **Best Student Paper Award** at the 14th USENIX Security Symposium, Security Analysis of a Cryptographically Enabled RFID Device (with Stephen C. Bono, Matthew Green, Ari Juels, Adam Stubblefield, Michael Szydlo).
- 2004 Electronic Frontiers Foundation **Pioneer Award**.
- **Baltimorean of the Year**, Baltimore Magazine, January, 2004.
- 2001 Index on Censorship **Freedom of Expression Award** for the Best Circumvention of Censorship for the Publius project.
- 2000 **Best Paper Award** at the 9th USENIX Security Symposium, A robust, tamper-evident and censorship-resistant web publishing system (with Marc Waldman and Lorrie Cranor).
- 1999 **Best Paper Award & Best Student Paper Award** at the 8th USENIX Security Symposium, The Design and Analysis of Graphical Passwords (with Ian Jermyn, Alain Mayer, Fabian Monrose, and Michael K. Reiter).
- 1996 Coauthor of **Best Student Paper**, Building Systems that Flexibly Control Downloaded Executable Content, at the 6th USENIX UNIX Security Symposium. Student: Trent Jaeger.
- 1992 National Science Foundation **Fellowship Summer Institute in Japan**
- 1986 **Branstrom Prize**, University of Michigan

Technical Advisory Boards

Current Positions

Qualytics: Data Quality Assurance

RunSafe: Binary rewriting to protect software

MarinaLife: Online boat slip bookings

Past Technical Advisory Board Positions with Successful Exits

Arbor Networks: Acquired by Danaher, August, 2010.

Authentica: Acquired by EMC Corporation, March, 2006.

Fortify Software: Acquired by Hewlett Packard, September 2010.

Gilian Technologies: Acquired by Breach Security, Inc, July, 2004.

Hx Technologies: Acquired by MEDecision, May, 2009.

Indigo Security: Acquired by Tablus, February, 2005.

NeoPath Networks: Acquired by Cisco, April, 2007.

Netscaler: Acquired Citrix Systems, August, 2005.

SiteAdvisor: Acquired by McAfee, April, 2006.

Tablus: Acquired by EMC Corporation, August, 2007.

ZeroFox: Public Offering via SPAC, July, 2022.