

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ROKU, INC. and VIZIO, INC.,
Petitioners

v.

ANCORA TECHNOLOGIES INC.,
Patent Owner

Case IPR2021-01406
U.S. Patent No. 6,411,941

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 6,411,941**

Mail Stop “PATENT BOARD”
Patent Trial and Appeal Board
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	MANDATORY NOTICES	4
III.	REQUIREMENTS FOR <i>INTER PARTES</i> REVIEW.....	7
A.	Grounds for Standing	7
B.	Overview of Challenge and Relief Requested	7
1.	Identification of Prior Art	7
2.	Grounds for Challenge.....	8
3.	Statutory Grounds of Challenge and Legal Principles	8
IV.	DESCRIPTION OF TECHNOLOGY	9
A.	Overview of the Technology.....	9
B.	Overview of the '941 Patent.....	10
1.	The Specification and Alleged Invention	11
2.	Prosecution History and Later Proceedings.....	16
3.	The Challenged Claims.....	19
V.	CLAIM CONSTRUCTION	20
VI.	LEVEL OF ORDINARY SKILL IN THE ART.....	21
VII.	SPECIFIC GROUNDS FOR PETITION.....	22
A.	Ground I: Claims 1-2, 11, and 13 were obvious over the combined teachings of Hellman and Chou.	22
1.	Overview of Hellman.....	22
2.	Overview of Chou.....	27
3.	Motivations to Combine Hellman and Chou	28
4.	Claim 1 preamble: “A method of restricting software operation within a license for use with a computer including an erasable, non-volatile memory area of a BIOS of the computer, and a volatile memory area; the method comprising the steps of:” ...	33
5.	Claim 1.a: “selecting a program residing in the volatile memory,”	36
6.	Claim 1.b: “using an agent to set up a verification structure in the erasable, non-volatile memory of the BIOS, the verification structure accommodating data that includes at least one license	

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

	record,”	38
7.	Claim 1.c: “verifying the program using at least the verification structure from the erasable non-volatile memory of the BIOS, and”	39
8.	Claim 1.d: “acting on the program according to the verification.”	40
9.	Claim 2: “A method according to claim 1, further comprising the steps of: establishing a license authentication bureau.”	40
10.	Claim 11: “A method according to claim 1 wherein the volatile memory is a RAM.”	41
11.	Claim 13: “The method of claim 1, wherein a unique key is stored in a first non-volatile memory area of the computer.” ...	41
B.	Ground II: Claims 1-3, 6-14, and 16 were obvious over the combined teachings of Hellman, Chou, and Schneck.....	42
1.	Overview of Schneck.....	42
2.	Motivations to Combine Hellman, Chou, and Schneck	43
3.	Claim 1. preamble: “A method of restricting software operation within a license for use with a computer including an erasable, non-volatile memory area of a BIOS of the computer, and a volatile memory area; the method comprising the steps of:” ...	46
4.	Claim 1.a: “selecting a program residing in the volatile memory,”	47
5.	Claim 1.b: “using an agent to set up a verification structure in the erasable, non-volatile memory of the BIOS, the verification structure accommodating data that includes at least one license record,”	48
6.	Claim 1.c: “verifying the program using at least the verification structure from the erasable non-volatile memory of the BIOS, and”	50
7.	Claim 1.d: “acting on the program according to the verification.”	51
8.	Claim 2: “A method according to claim 1, further comprising the steps of: establishing a license authentication bureau.”	51
9.	Claim 3 preamble: “A method according to claim 2, wherein setting up a verification structure further comprising the steps	

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

	of:”	51
10.	Claim 3.a: “establishing, between the computer and the bureau, a two-way data-communications linkage;”	51
11.	Claim 3.b: “transferring, from the computer to the bureau, a request-for-license including an identification of the computer and the license-record’s contents from the selected program;”	52
12.	Claim 3.c: “forming an encrypted license-record at the bureau by encrypting parts of the request-for-license using part of the identification as an encryption key;”	55
13.	Claim 3.d: “transferring, from the bureau to the computer, the encrypted license-record; and”	55
14.	Claim 3.e: “storing the encrypted license record in the erasable non-volatile memory area of the BIOS.”	56
15.	Claim 6: “A method according to claim 1 wherein selecting a program includes the steps of: establishing a licensed-software-program in the volatile memory of the computer wherein said licensed-software-program includes contents used to form the license-record.”	56
16.	Claim 7 preamble: “A method according to claim 6 wherein using an agent to set up the verification structure includes the steps of:”	56
17.	Claim 7.a: “establishing or certifying the existence of a pseudo-unique key in a first non-volatile memory area of the computer; and”	57
18.	Claim 7.b: “establishing at least one license-record location in the first nonvolatile memory area or in the erasable, non-volatile memory area of the BIOS.”	57
19.	Claim 8 preamble: “A method according to claim 6 wherein establishing a license-record includes the steps of:”	58
20.	Claim 8.a: “forming a license-record by encrypting of the contents used to form a license-record with other predetermined data contents, using the key; and”	58
21.	Claim 8.b: “establishing the encrypted license-record in one of the at least one established license-record locations.”	58
22.	Claim 9 preamble: “A method according to claim 7 wherein verifying the program includes the steps of:”	59

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

23.	Claim 9.a: “encrypting the licensed-software-program's license-record contents from the volatile memory area or decrypting the license-record in the erasable, non-volatile memory area of the BIOS, using the pseudo-unique key; and”	59
24.	Claim 9.b: “comparing the encrypted licenses-software-program’s license-record contents with the encrypted license-record in the erasable, non-volatile memory area of the BIOS, or comparing the license-software-program's license-record contents with the decrypted license-record in erasable non-volatile memory area of the BIOS.”	60
25.	Claim 10: “A method according to claim 9 wherein acting on the program includes the step: restricting the program's operation with predetermined limitations if the comparing yields non-unity or insufficiency.”	61
26.	Claim 11: “A method according to claim 1 wherein the volatile memory is a RAM.”	61
27.	Claim 12: “The method of claim 1, wherein a pseudo-unique key is stored in the non-volatile memory of the BIOS.”	62
28.	Claim 13: “The method of claim 1, wherein a unique key is stored in a first non-volatile memory area of the computer.” ...	63
29.	Claim 14: “The method according claim 13, wherein the step of using the agent to set up the verification record, including the license record, includes encrypting a license record data in the program using at least the unique key.”	63
30.	Claim 16: “The method according to claim 13, wherein the step of verifying the program includes a decrypting the license record data accommodated in the erasable second non-volatile memory area of the BIOS using at least the unique key.”	63
VIII.	THE BOARD SHOULD <u>NOT</u> EXERCISE ITS DISCRETION UNDER §§ 325(d) and 314(a) TO DENY REVIEW.	64
A.	<u>The substance of this Petition does not warrant denial under § 325 (d).</u>	64
B.	The substance of this Petition also does not warrant denial under § 314(a).....	65
1.	The <i>General Plastic</i> factors favor institution.....	65
2.	The <i>Fintiv</i> factors favor institution.	68

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

IX. CONCLUSION.....70

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

PETITIONER’S EXHIBIT LIST

Exhibit No.	Description
1001	U.S. Patent No. 6,411,941 to Mullor et al. (“’941 Patent”)
1002	Image File Wrapper of U.S. Patent No. 6,411,941 (“’941 Patent File History”)
1003	Declaration of Andrew Wolfe, Ph.D. (“Wolfe Decl.”)
1004	U.S. Patent No. 4,658,093 (“Hellman”)
1005	U.S. Patent No. 5,892,906 (“Chou”)
1006	U.S. Patent No. 5,933,498 (“Schneck”)
1007	Scheduling Order, <i>Ancora Techs., Inc. v. TCT Mobile (US), Inc.</i> , No. 8:19-cv-2192 (C.D. Cal. Mar. 17, 2020) (ECF No. 34)
1008	In re: Coronavirus Public Emergency, Order Concerning Phased Reopening of the Court, General Order No. 20-09, United States District Court for the Central District of California, Aug. 6, 2020
1009	Civil Docket, <i>Ancora Techs., Inc. v. Sony Mobile Commc’ns AB</i> , No. 1:19-cv-01703 (D. Del.)
1010	Civil Docket, <i>Ancora Techs., Inc. v. Lenovo Grp. Ltd.</i> , No. 1:19-cv-01712 (D. Del.)
1011	Claim Construction Order, <i>Ancora Techs., Inc. v. Apple Inc.</i> , No. 4:11-cv-06357 (N.D. Cal. Dec. 31, 2012) (ECF No. 107)
1012	Final Claim Constructions of the Court, <i>Ancora Techs., Inc. v. LG Elecs., Inc.</i> , No. 1:20-cv-00034 (W.D. Tex. June 2, 2020) (ECF No. 69)
1013	Supplemental Claim Construction Order, <i>Ancora Techs., Inc. v. LG Elecs., Inc.</i> , No. 1:20-cv-00034 (W.D. Tex. Aug. 19, 2020) (ECF No. 93)
1014	Joint Claim Construction and Prehearing Statement, <i>Ancora Techs., Inc. v. TCT Mobile (US), Inc.</i> , No. 8:19-cv-2192 (C.D. Cal. July 17, 2020) (ECF No. 49)
1015	European Patent Application No. EP 0766165A2 (“’165 Application”)
1016	U.S. Patent No. 5,724,425 (“’425 Patent”)
1017	U.S. Patent No. 6,138,236 (“’236 Patent”)
1018	U.S. Patent No. 5,802,592 (“’592 Patent”)
1019	U.S. Patent No. 5,835,594 (“’594 Patent”)

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

Exhibit No.	Description
1020	Telephonic Markman Hearing, <i>Ancora Techs., Inc. v. TCT Mobile (US), Inc., et al.</i> , No. 8:19-cv-2192 (C.D. Cal. Oct. 15, 2020) (ECF No. 60)
1021	Telephonic Markman Hearing, <i>Ancora Techs., Inc. v. TCT Mobile (US), Inc., et al.</i> , No. 8:19-cv-2192 (C.D. Cal. Oct. 15, 2020) (ECF No. 69)
1022	Complaint, <i>Ancora Techs., Inc. v. TCL Corp., et al.</i> , No. 4:19-cv-00624 (E.D. Tex. Aug. 27, 2019) (ECF No. 1)
1023	U.S. Patent No. 5,734,819 (“Lewis”)
1024	File Wrapper of <i>Ex Parte</i> Reexamination of U.S. Patent No. 6,411,941, Control No. 90/010,560 (“’560 Reexam File Wrapper”)

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

Petitioners request *inter partes* review of U.S. Patent No. 6,411,941 (EX1001).

I. INTRODUCTION

The '941 Patent generally relates to methods for restricting unauthorized software operation. Specifically, the claimed method stores a license record in a BIOS memory, which purportedly overcame deficiencies using a software-based prior art method where a license record was stored in “volatile memory (*e.g.*, hard disk)” and a hardware-based prior art method. EX1001, '941 Patent, 1:10-42. Indeed, storing a license record for a program in the BIOS memory, and not just any non-volatile memory, is the supposed improvement of the '941 Patent claims, as Patent Owner has argued during prosecution, an *ex parte* reexamination, covered business method reviews, and two Federal Circuit appeals. But by 1998, the earliest priority date of the '941 Patent, the storage of license records in a BIOS memory was not a patentable distinction, as Petitioners demonstrate via three prior art references to Hellman (EX1004), Chou (EX1005), and Schneck (EX1006).

The '941 Patent has been litigated in district court and at the Patent Office in numerous cases. *See* Sec. II. *infra*. But its invalidity over Hellman, Chou and Schneck has never been fully resolved. Neither of the Federal Circuit appeals considered prior art invalidity—one appeal was limited to claim construction issues, and one appeal was limited to patent eligibility. The prior covered business

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

method reviews were denied institution on the basis that the '941 Patent was not eligible for covered business method review. And for the two *inter partes* review proceedings that the Board previously instituted over Hellman, Chou and Schneck, the parties reached a settlement agreement and the IPR proceedings were subsequently terminated without a trial. Despite the Patent Owner having asserted the '941 Patent against 10 entities over the course of more than 10 years, the invalidity of the '941 Patent's claims has only been considered on the merits in one instance—an *ex parte* reexam that did not consider Hellman, Chou, or Schneck.

This Petition presents the same grounds on which the Board has recently instituted *inter partes* review of the '941 patent. Specifically, in February 2021, the Board instituted review of a petition filed by, among others, TCT Mobile (US), Inc. *See TCT Mobile (US) Inc. v. Ancora Techs., Inc.* IPR2020-01609, Paper 7 (P.T.A.B. Feb. 16, 2021). Shortly after institution, a number of entities filed “me too” petitions, including one petition by several Sony entities. *See Sony Mobile Commc'ns AB v. Ancora Techs., Inc.*, IPR2021-00663, Paper 1 (P.T.A.B. Mar. 15, 2021). Sony moved to join the TCT Mobile proceeding. *Sony*, Paper 4 (Mar. 15, 2021). In June 2021, the Board instituted Sony's petition for *inter partes* review and granted Sony's joinder motion.¹ *TCT Mobile*, Paper 25 (July

¹ For various reasons not relevant here, the Board denied joinder motions by HTC Corporation and LG Electronics. *HTC Corp. v. Ancora Techs. Inc.*, IPR2021-

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

16, 2021); *Sony*, Paper 17 (June 16, 2021). The parties to both the Sony and TCT Mobile IPRs subsequently settled with Patent Owner Ancora and, on July 16, 2021, the Board granted the parties joint motions to terminate the joined IPR proceedings. *Sony*, Paper 20 (July 16, 2021). Ancora subsequently sued Roku and VIZIO (and others) for infringement later that same day.

There have been no intervening events following the termination of the TCT Mobile and Sony petitions that impact the patentability of the challenged claims of the '941 patent or the reasoning applied by the Board in instituting the TCT Mobile and Sony petitions. Those institution decisions analyzed the exact same grounds presented here and the institution rationale should apply with full force. Petitioners submit that the prior art demonstrates that storing information, a license record or otherwise, in the BIOS memory, that is used in a method to restrict unauthorized operation of software, was well-known as a way to provide increased protection against tampering with that information by, for example, a software hacker.

00570, Paper 17 at 8-14 (P.T.A.B. June 10, 2021) (finding that a majority of factors under *General Plastic* weighed against institution because of HTC's prior filed CBM petition); *LG Elecs., Inc. v. Ancora Techs., Inc.*, IPR2021-00581, Paper 16 at 8-12 (P.T.A.B. June 10, 2021) (finding that a majority of factors under *Fintiv* weighed against institution based on the advanced stages of the parallel district court proceeding).

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

Petitioners demonstrate through the combinations of Hellman, Chou, and Schneck that a person of ordinary skill in the art at the time of the invention (POSA) would have found all challenged claims obvious.

For the reasons described herein and the reasons articulated by the Board in its prior institution decisions over the same grounds, Petitioners request institution of this *inter partes* review petition and cancellation of all challenged claims.

II. MANDATORY NOTICES

REAL PARTY-IN-INTEREST: Roku, Inc. and VIZIO, Inc. are the real parties-in-interest.

RELATED MATTERS: Patent Owner has asserted the '941 Patent against Roku and VIZIO in the following district-court litigations:

- *Ancora Technologies, Inc. v. Roku, Inc.*, Case No. 6:21-cv-00737 (W.D. Tex.), filed July 16, 2021; and
- *Ancora Technologies, Inc. v. VIZIO, Inc.*, Case No. 6:21-cv-00739, filed July 16, 2021.

Petitioners are aware of the following additional district court litigations involving the '941 Patent:

- *Ancora Technologies, Inc. v. Lenovo Group Limited*, Case No. 1:19-cv-01712 (D. Del.), filed September 12, 2019;
- *Ancora Technologies, Inc. v. Samsung Electronics Co., Ltd.*, Case No.

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

6:19-cv-00385 (W.D. Tex.), filed June 21, 2019;

- *Ancora Technologies, Inc. v. HTC America, Inc.*, Case No. 2:16-cv-01919 (W.D. Wash.), filed December 15, 2016;
- *Ancora Technologies, Inc. v. LG Electronics, Inc.*, Case No. 6:21-cv-00561 (W.D. Tex.), filed June 21, 2019;
- *Ancora Technologies, Inc. v. Google, LLC*, Case No. 6:21-cv-00735 (W.D. Tex.), filed July 16, 2021; and
- *Ancora Technologies, Inc. v. Nintendo Co., Ltd.*, Case No. 6:21-cv-00738 (W.D. Tex.), filed July 16, 2021.

The '941 Patent has been challenged at the Patent Trial and Appeal Board in the following proceedings:

Case	Proceeding No.	Filed	Status
<i>Apple Inc. v. Ancora Technologies Inc.</i>	CBM2016-00023	January 8, 2016	Institution Denied
<i>HTC America, Inc. v. Ancora Technologies Inc.</i>	CBM2017-00054	May 26, 2017	Institution Denied
<i>Samsung Electronics Co., Ltd. v. Ancora Technologies, Inc.</i>	IPR2020-01184	June 25, 2020	Institution Denied
<i>TCT Mobile (US) Inc. v. Ancora Technologies, Inc.</i>	IPR2020-01609	September 10, 2020	Terminated After Institution
<i>Samsung Electronics Co., Ltd. v. Ancora Technologies, Inc.</i>	IPR2021-00583	February 24, 2021	Dismissed Prior to Institution

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

Case	Proceeding No.	Filed	Status
<i>Sony Mobile Communications, AB v. Ancora Technologies, Inc.</i>	IPR2021-00663	March 15, 2021	Terminated After Institution
<i>HTC Corporation v. Ancora Technologies, Inc.</i>	IPR2021-00570	February 19, 2021	Institution Denied
<i>LG Electronics, Inc. v. Ancora Technologies, Inc.</i>	IPR2021-00581	February 23, 2021	Institution Denied
<i>Nintendo Co., Ltd. v. Ancora Technologies, Inc.</i>	IPR2021-01338	August 10, 2021	Pending

The '941 Patent was subject to *Ex Parte* Reexamination Control No. 90/010,560, filed May 29, 2009. An *Ex Parte* Reexamination Certificate was issued on June 1, 2010, adding no claims and making no amendments to the '941 Patent.

LEAD AND BACKUP COUNSEL: Under 37 C.F.R. §§ 42.8(b)(3) and 42.10(a), Petitioners appoint Jon E. Wright (Reg. No. 50,720) as lead counsel and Lestin L. Kenton (Reg. No. 72,314) and Dohm Chankong (Reg. No. 70,524) as back-up counsel, each at the address: STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C., 1100 New York Avenue, N.W., Washington, D.C., 20005, phone (202) 371-2600, and facsimile (202) 371-2540.

SERVICE INFORMATION: Petitioners consent to electronic service by email at jwright-PTAB@sternekessler.com, lkenton-PTAB@sternekessler.com,

dchankong-PTAB@sternekessler.com, and PTAB@sternekessler.com.

III. REQUIREMENTS FOR *INTER PARTES* REVIEW

A. Grounds for Standing

Petitioners certify that the '941 Patent is available for IPR and that Petitioners are not barred or estopped from requesting IPR challenging claims of the '941 Patent on the grounds presented here.

B. Overview of Challenge and Relief Requested

Petitioner requests cancellation of claims 1-3, 6-14, and 16 of the '941 Patent under pre-AIA 35 U.S.C. § 103. The grounds presented here are the same as the grounds presented in both the instituted TCT Mobile petition, *TCT Mobile*, Paper 1 at 21-63, the instituted Sony petition, *Sony*, Paper 1 at 20-60, and the grounds requested by Nintendo in IPR2021-01338.

1. Identification of Prior Art

Petitioners rely upon the references listed in the Table of Exhibits, including: U.S. Patent No. 4,658,093 (EX1004, "Hellman"), issued on April 14, 1987, from an application filed on July 11, 1983. Hellman is prior art under pre-AIA 35 U.S.C. § 102(b).

U.S. Patent No. 5,892,906 (EX1005, "Chou"), issued on April 6, 1999, from an application filed on July 19, 1996. Chou is prior art under pre-AIA 35 U.S.C. § 102(e).

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

U.S. Patent No. 5,933,498 (EX1006, “Schneck”), issued on August 3, 1999, from an application filed on November 5, 1997, and that claims priority to an application filed on January 11, 1996. Schneck is prior art under pre-AIA 35 U.S.C. § 102(e).

Hellman, Chou, and Scheck were neither presented to nor discovered by the Patent Office during the original examination, the *ex parte* reexamination, or the covered business method review of the ’941 Patent. Hellman, Chou, and Schneck form the basis for the grounds set forth in the instituted TCT Mobile and Sony IPRs, which were subsequently terminated after settlement. *See* Sec. I. *supra*.

2. Grounds for Challenge

Ground	Basis	Reference(s)	Challenged Claims
1	§ 103	Hellman, Chou	1-2, 11, 13
2	§ 103	Hellman, Chou, Schneck	1-3, 6-14, and 16

This Petition and the Dr. Andrew Wolfe Declaration (EX1003, “Wolfe Decl.”) demonstrate a reasonable likelihood that Petitioner will prevail with respect to cancellation of at least one challenged claim. *See* 35 U.S.C. § 314(a). Dr. Wolfe submitted a substantively similar supporting declarations in the instituted TCT Mobile petition, *TCT Mobile*, EX1003 (Sept. 10, 2020) and Nintendo’s IPR against the ’941 Patent.

3. Statutory Grounds of Challenge and Legal Principles

This Petition requests cancellation of claims 1-3, 6-14, and 16 of the ’941

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

Patent under pre-AIA 35 U.S.C. § 103. The grounds presented here are the same as the grounds presented in both the instituted (but terminated) TCT Mobile petition, *TCT Mobile*, Paper 1 at 21-63, and the instituted (but terminated) Sony petition, *Sony*, Paper 1 at 20-60. The grounds here are also the same as those requested by Nintendo in IPR2021-01338, filed August 10, 2021.

IV. DESCRIPTION OF TECHNOLOGY

A. Overview of the Technology

By the time of the '941 Patent's priority date in 1998, the field of software licensing was well-developed. EX1003, Wolfe Decl., ¶¶31-35. For more than a decade prior, practitioners in the field had widely recognized the new risks to software piracy introduced by the transformations to digital media. *Id.*

Many entities recognized that one such risk was “copy protection” or “secondary distribution.” *Id.* This referred to the situation where a user received a valid license for a software program, but the user then duplicated the program and/or the license so as to use it in an unauthorized fashion for more uses, on more computers, etc. *Id.* This problem was of particular interest to practitioners because it required the software owner to provide enough trust to the user to perform at least one authorized use, as opposed to providing no trust or unlimited trust. *Id.* While many solutions were developed, a common theme was to use some form of encryption to reduce unauthorized secondary distribution of the software program.

Id.

Similarly, by 1998, the field of computer BIOS was well-developed. EX1003, ¶¶36-42. Nearly all consumer end user devices contained a BIOS program that was used to start up the device at power-on time. *Id.* Early personal computers tended to store BIOS programs in separate, true ROM (read only memory) memory module, i.e., memory that could not be re-written in the field. *Id.* By the 1990s, it was more common to store BIOS programs in “ROM” that could actually be rewritten in some form. *Id.* Early forms of this rewritable ROM often required physically accessing the memory chip with a special device. *Id.*

By the '941 Patent's priority date in 1998, electrically-erasable programmable read-only memory (EEPROM) was a popular medium for BIOS memory. *Id.* EEPROM chips had the benefit of being re-writable by software without the need to remove the chip from the computer. *Id.* This aspect of EEPROM was considered beneficial because it became common prior to the '941 priority date in 1998 for device manufacturers to provide updates to BIOS while the devices were in the field. *Id.* EEPROM allowed that functionality. *Id.*

B. Overview of the '941 Patent

The '941 Patent issued from U.S. Patent Application No. 09/164,777, filed on October 1, 1998. It claims priority to Israeli Patent Application 124571, which was filed on May 21, 1998. EX1001, Cover Page. Therefore, the priority date of

the '941 Patent is no earlier than May 21, 1998.

1. The Specification and Alleged Invention

The '941 Patent invention is directed to “restricting an unauthorized software program’s operation.” EX1001, 1:6-8. The '941 Patent recognizes that it was known in the field to store a “license signature” for a program in a computer’s “volatile memory (*e.g.* hard disk).”² *Id.*, 1:19-21. The '941 Patent alleges that such techniques were “appropriate for restricting honest software users,” but they were “vulnerable to attack at the hands of skilled system’s programmers (*e.g.*, ‘hackers’).” *Id.*, 1:21-24.

The '941 Patent proposes to solve this problem based on “the use of a key and of a record, which have been written into the non-volatile memory of a computer.” *Id.*, 1:38-43. The “key” is stored “during manufacture” in a “ROM section” of a “BIOS module,” and it “constitutes, effectively, a unique identification code for the host computer.” *Id.*, 1:44-52. The “license record” is stored in “another (second) non-volatile section of the BIOS, *e.g.*, E2PROM (or the

² Despite this contradictory example (i.e., that a hard disk is exemplary of volatile memory), the Federal Circuit held that “volatile memory” has its ordinary meaning, *Ancora Technologies, Inc. v. Apple, Inc.*, 744 F.3d 732, 739 (Fed. Cir. 2014), such as “memory whose data is not maintained when the power is removed,” *id.*, 737.

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

ROM).”³ *Id.*, 1:59-2:1. The ’941 Patent distinguishes the storage location of the key and the license record: “It should be noted that unlike the first non-volatile section, the data in the second non-volatile memory may optionally be erased or modified (using E2PROM manipulation commands), so as to enable to add, modify or remove licenses.” *Id.* 2:1-5. The key is used to encrypt the license record, creating a locally stored, device-specific license record for the program under license. *Id.*, 1:59-2:26.

The ’941 Patent alleges two primary benefits of the invention. First, by encrypting the license record with a key unique to the host computer and stored in ROM, a program licensed for one computer cannot simply be transferred with the license record to another computer, because the key for the second computer will be different. *Id.*, 2:27-47. “It is important to note that the hacker is unable to modify the key in the ROM of the second computer to” the key of the first computer because “the contents of the ROM is established during manufacture and is practically invariable.” *Id.*, 2:42-47.

Second: “An important advantage in utilizing non-volatile memory such as that residing in the BIOS is that the required level of system programming expertise that is necessary to intercept or modify commands, interacting with the BIOS, is substantially higher than those needed for tampering with data residing in

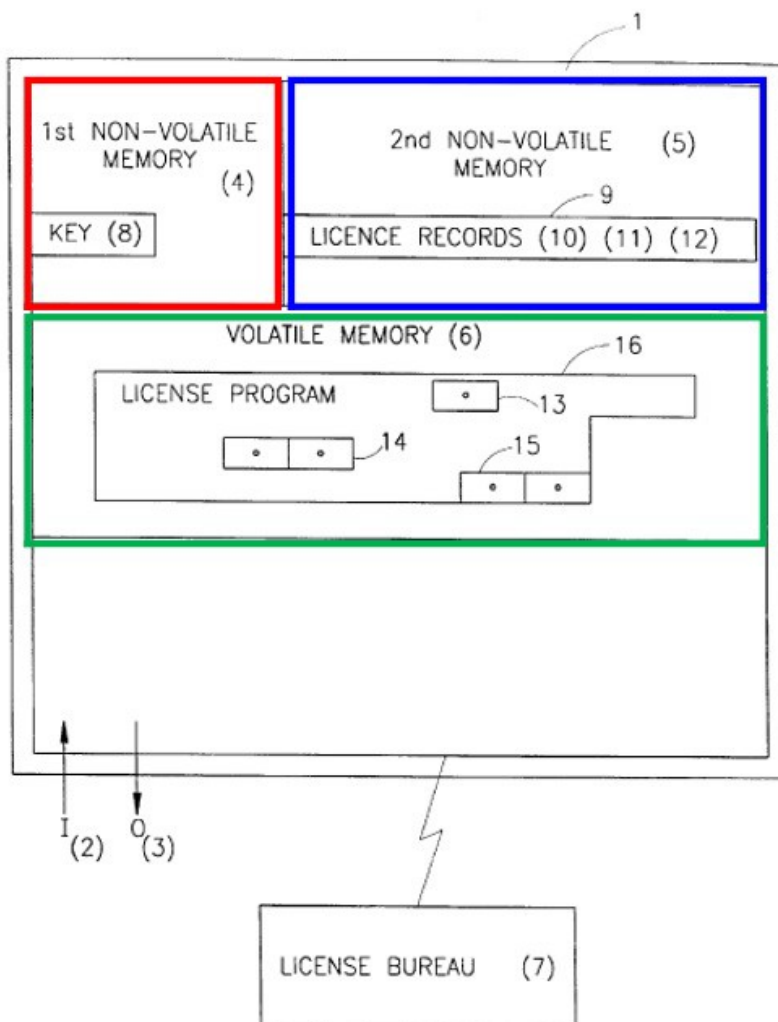
³ E2PROM is another spelling of EEPROM.

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

volatile memory such as hard disk.” *Id.*, 3:4-9. In other words, because manipulation of E2PROM was more difficult than manipulation of the device’s RAM or hard disk, the license record could be stored in E2PROM to make it more tamper proof. *Id.*, 3:4-17.

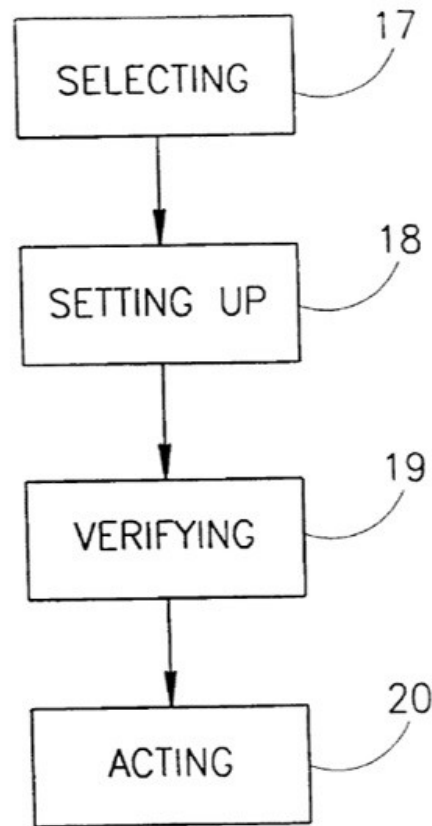
The alleged invention is depicted with respect to Figure 1 of the ’941 Patent, shown below. The **first non-volatile memory** (4)—“e.g. the ROM section of the BIOS,” *id.*, 5:9-16—stores a key (8). The **second non-volatile memory** (5)— “e.g. the E2PROM section of the BIOS,” *id.*—stores license records (10, 11, 12).

The **volatile memory** (6)—“e.g. the internal RAM memory of the computer,” *id.*— stores a license program (16).



EX1001, FIG. 1 (annotated).

With respect to Figure 2, shown below, the '941 Patent describes a method for using the structures described above to effectuate the alleged invention.



EX1001, FIG. 2.

At the selecting (17) step, “a licensed-software-program” is established in the volatile memory.” *Id.*, 6:7-16.

At the setting up (18) step, a “pseudo-unique key” is established (or certified to already exist) in the first non-volatile memory. *Id.*, 6:18-21. Further, a “license-record location” is established in the first or the second non-volatile memory area,” *id.*, which action includes using the key to form an “encrypted license-record” in the license-record location, *id.*, 6:22-27.

At the verifying (19) step, the license record established in the license-record location is compared to a result of using the key to encrypt information from the

licensed-software-program. *Id.*, 6:28-39.

At the acting (20) step, an action, such as “restricting the program’s operation,” is performed in response to the comparison from the verifying (19) step, such as if the comparison shows the two values are unequal. *Id.*, 6:40-52.

Thus, using the structures described with respect to Figure 1 and the process described with respect to Figure 2, the ’941 Patent’s alleged invention is providing a license record unique to a specific computer and stored in a harder-to-modify memory device, BIOS memory, such as BIOS E2PROM, and not just any non-volatile memory. With these aspects, the invention allowed device-specific, more tamperproof software licensing.

2. Prosecution History and Later Proceedings

Claim 1 as originally filed covered setting up a verification structure in two non-volatile memories, and verifying a program in volatile memory based thereon. *See* ’941 File Wrapper, Claims, dated Oct. 1, 1998, p. 1.

During prosecution, the Applicant amended claim 1 to change the “setting up ...” step to a “using an agent to set up ...” step. *See* ’941 File Wrapper, Office Action Response, dated Dec. 6, 2001, p. 10 (unnumbered page following page 9). The Applicant also amended the claims to recite, as in its ultimately issued form, that the verification structure was stored “in the erasable, non-volatile memory of the BIOS.” *Id.* The Applicant later argued that this storing of the license record in

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

the memory of the BIOS was what distinguished claim 1 over the prior art of record. See EX1002, '941 File Wrapper, 0197-0201. The Applicant alleged that this storage in the memory of the BIOS was unknown in the prior art both because “[t]here is no OS support whatsoever to write data to the system BIOS,” and because “no file system is associated with the BIOS.” *Id.*, 0200.

The Examiner allowed the claims based on this distinction. The prior art of record disclosed, for instance, a licensing software that stored licenses in a device’s ordinary “persistent non-volatile storage,” *Id.*, 0212 (citing U.S. Pat. No. 6,189,146, 12:8-31), and “the use of BIOS memory for storing licensing numbers,” *id.*, 0213 (citing U.S. Pat. No. 5,479,639). But, according to the Examiner, the prior art failed to show “licensed programs running at the OS level interacting with a program verification structure stored in the BIOS ... [.]” *Id.* “Further, it is well known to those of ordinary skill of the art that a computer BIOS is not setup to manage a software license verification structure.” *Id.* According to the Examiner, the '941 Patent solved that problem by using the “agent” to set up the verification structure in the memory of the BIOS. *Id.*

The '941 Patent was subject to an *ex parte* reexamination identified by Control Number 90/010,560. The prior art submitted by the requester, U.S. Pat. No. 5,734,819 (“Lewis”), did disclose license information stored in the non-volatile memory of a BIOS. See EX1024, '560 Reexam File Wrapper, 0249. But

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

the Examiner found that Lewis fell short of disclosing claim 1 because the system in Lewis used the license information to verify the ***device itself***, not a program running on the device. *Id.*, 0249-0250. That is, in Lewis, the program used the encrypted license information in the BIOS memory to verify that the serial number of the device had not been altered, instead of using the encrypted license information to verify that the program was licensed. *See* EX1023, Lewis, 3:16-36, 5:10-26. For this reason, the Examiner allowed issuance of the reexamination certificate. *See* EX1024, 0249-0250.

The '941 Patent was subject to a covered business method review. The Board denied institution, finding that the '941 Patent was not a covered business method patent because it disclosed a technical solution in the form of storing the license record in the memory of the BIOS. *HTC Corp. v. Ancora Techs., Inc.*, CBM2017-00054, Paper 7 at 10-12 (P.T.A.B. Dec. 1, 2017). The Board therefore did not consider the merits of the prior art-based invalidity grounds present in the CBM petition.

The '941 Patent was subject to an appeal to the Federal Circuit in *Ancora Technologies, Inc. v. Apple, Inc.*, 744 F.3d 732 (Fed. Cir. 2014). Addressing a claim construction ruling by the district court, the Federal Circuit held that (1) the recited “program” was not limited to only ***application*** programs, *id.* at 734-37, and that (2) the confused language in the specification regarding “volatile memory”

and “non-volatile memory” did not render those terms indefinite in light of their well-known conventional meaning, *id.* at 737-39.

The '941 Patent was subject to another appeal to the Federal Circuit in *Ancora Technologies, Inc. v. HTC Am., Inc.*, 908 F.3d 1343 (Fed. Cir. 2018). Reviewing a district court ruling on the pleadings that the claims of the '941 Patent were patent ineligible, the Federal Circuit reversed. The court found that, at step 1 of the *Alice* analysis, claim 1 was not directed to an abstract idea. *Id.* at 1348-49. The court found that claim 1 was directed to an improvement to computer security with its alleged improvement of “a structure containing a license record is stored in a particular, modifiable, non-volatile portion of the computer’s BIOS, and the structure in that memory location is used for verification by interacting with the distinct computer memory that contains the program to be verified.” *Id.* On the pleadings, the court did not find any reason to dispute the '941 Patent’s assertion that this storage in BIOS memory resulted in a “beneficial reduction of the risk of hacking.” *Id.* at 1349.

3. The Challenged Claims

Claim 1, the only independent claim challenged in this Petition, recites:

1. A method of restricting software operation within a license for use with a computer including an erasable, non-volatile memory area of a BIOS of the computer, and a volatile memory area; the method comprising the steps of:

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

- [a] selecting a program residing in the volatile memory,
- [b] using an agent to set up a verification structure in the erasable, non-volatile memory of the BIOS, the verification structure accommodating data that includes at least one license record,
- [c] verifying the program using at least the verification structure from the erasable non-volatile memory of the BIOS, and
- [d] acting on the program according to the verification.

The remaining claims challenged in this Petition all depend directly or indirectly on Claim 1, and those claims are addressed in the grounds below.

V. CLAIM CONSTRUCTION

In an IPR proceeding, the challenged claims are construed “in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005) (*en banc*).

The claims of the '941 Patent have been construed by three courts as of the filing of this Petition: in *Ancora Techs., Inc. v. Apple Inc.*, No. 4:11-cv-06357 (N.D. Cal., J. Gonzalez Rogers) (*see* EX1011); in *Ancora Techs., Inc. v. LG Elecs., Inc.*, No. 1:20-cv-00034 (W.D. Tex., J. Albright) (*see* EX1012; EX1013); and in *Ancora Techs., Inc. v. TCT Mobile (US) Inc.*, No. 8:19-cv- 02192 (C.D. Cal., J. Wu) (*see* EX1020; EX1021, EX1014). No claim construction activities have yet

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

occurred in the parallel district court litigations between Petitioners and Patent Owner.

* * *

In instituting the TCT Mobile and Sony IPRs, the PTAB construed the term “license record” as “a record having information for verifying that licensed program.” *See TCT Mobile (US) Inc. v. Ancora Techs., Inc.*, IPR2020-01609, Paper 7 at 6-9 (P.T.A.B. Feb. 16, 2021). There, the Board rejected Ancora’s attempt to narrow the claims by reading an embodiment from the specification into the claims with its proposed construction of “license record” as “a record *from a licensed program* with information for verifying that licensed program.” *Id.* Should Patent Owner advocate again for this narrow construction, the Board should reject it under the same rationale expressed in the TCT Mobile proceeding. Petitioners do not believe that any additional claim constructions are needed for the purposes of this review.

VI. LEVEL OF ORDINARY SKILL IN THE ART

A person having ordinary skill in the art (“POSA”) at the time of the alleged invention would have had at least a B.S. degree in computer science, computer engineering, or electrical engineering (or equivalent experience) and would have had at least two years of experience with computer science and computer engineering, including information encryption, computer architecture, and

firmware programming. EX1003, ¶¶21-25. Additional educational experience could make up for less work experience and vice versa.

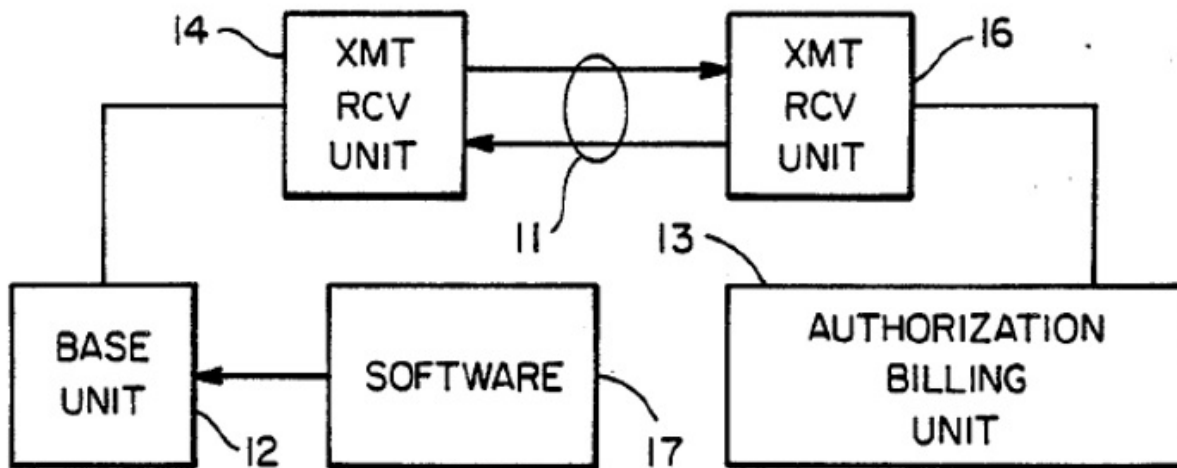
VII. SPECIFIC GROUNDS FOR PETITION

A. Ground I: Claims 1-2, 11, and 13 were obvious over the combined teachings of Hellman and Chou.

1. Overview of Hellman

Hellman, like the '941 Patent, disclosed a technique for using “base unit specific” software “authorizations” to limit the use of software, *e.g.*, “programs,” within the parameters defined by the software’s “manufacturer.” EX1004, Hellman, Abstract. Hellman disclosed that its technique “solves the ‘software piracy problem’.” *Id.*

In more detail, Hellman disclosed a system including a base unit 12, a software or “software package” 17, and an authorization billing unit 13. *Id.*, 5:39-50. The base unit 12 can be a computer. *See id.*, 2:24-27 (“acquaintances with similar base units (computers)”).

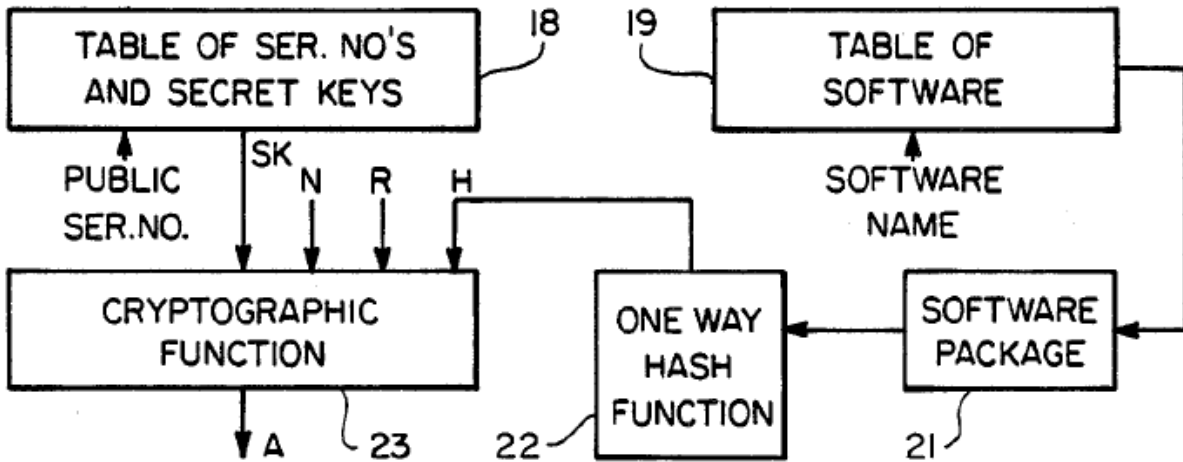


EX1004, FIG. 1.

“The user at base unit 12 obtains software package 17 by purchasing it at a store, over telephone line, or in some similar manner.” *Id.*, 5:51-53.

The base unit 12 sends to authorization and billing unit 13 a “user originated request for software use.” *Id.*, 5:57-59. The request includes the following information: software name (“the software package to be used”); serial number (“a serial number, identification number, user name or similar identifier unique to base unit 12”); N (“the number of additional uses of software requested”); R (“a random number”); and billing information. *Id.*, 5:57-6:2.

The authorization and billing unit 13 receives the request and will (presumably after billing the user) send back an authorization A. *Id.*, 6:3-8. The generation of that authorization A is described with respect to Figure 2, shown below.



EX1004, FIG. 2.

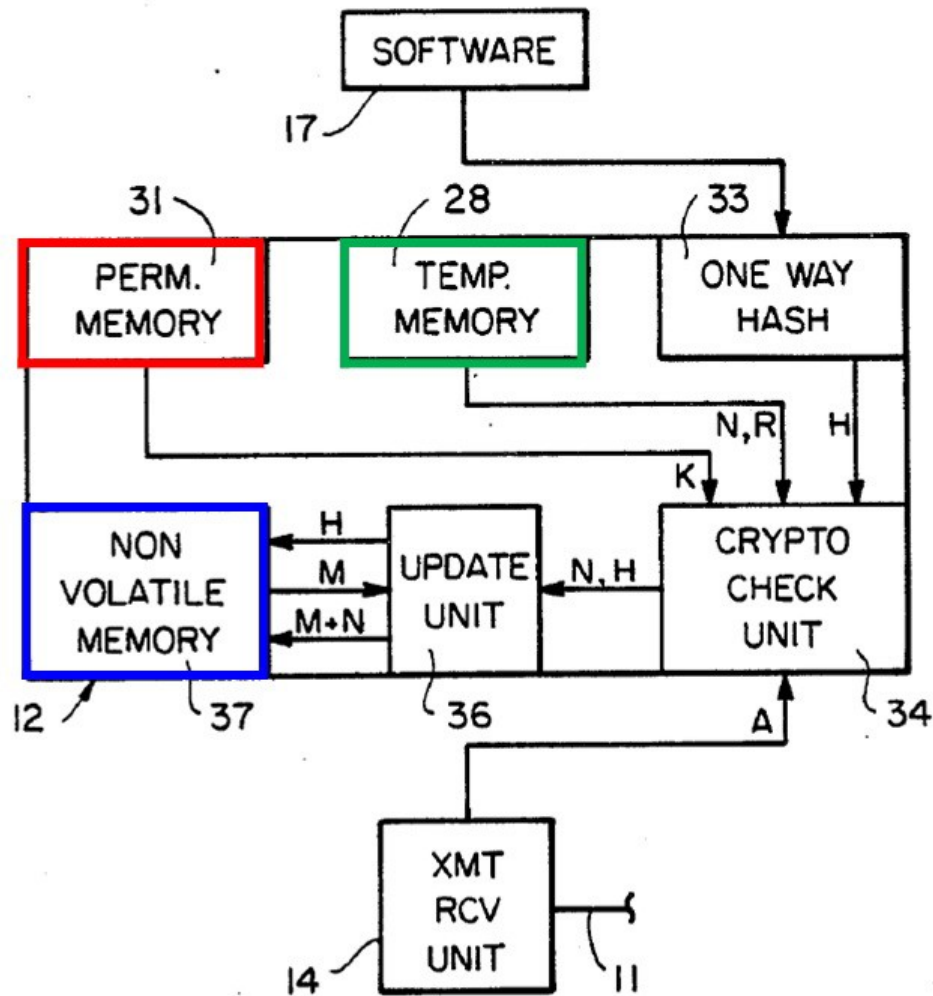
First, the authorization and billing unit 13 uses the received serial number for the base unit 12 to look up a shared secret key SK for the base unit 12. *Id.*, 6:17-21.

Second, the authorization and billing unit 13 uses the received software name to obtain software package 21, which is a duplicate of software package 17. *Id.*, 6:21-30. The authorization and billing unit 13 generates a cryptographic hash H based on the software package 21. *Id.*, 6:31-61. H is an “‘abbreviation’ or name for describing the software package 21” (and thus software package 17), and has the characteristic that it is easily calculated from software package 21, but software package 21 is not easily calculated from H. *Id.*, 6:33-42.

Third, the authorization and billing unit 13 inputs SK, H, N (the number of purchased uses), and R (the random number) into a cryptographic function. *Id.*, 6:62-7:2. Authorization A is the output of this cryptographic function, and A is

sent back to the base unit 12. *Id.*, 6:3-8, 6:62-7:2.

The result is that base unit 12 receives an authorization A which is unique to the licensed software package 17, unique to the base unit 12, and unique to the random number R. EX1003, ¶68. The use of authorization A by the base unit 12 is described with respect to Figure 6, shown below.



EX1004, FIG. 6 (annotated).

The base unit then also proceeds through a series of steps. First, the base unit 12 uses the software package 17 to generate the same cryptographic hash H. *Id.*

9:23-26.

Second, the base unit 12 retrieves key K from permanent memory 31. *Id.*, 9:29-40. For simplicity, K can be the same as SK. *Id.*, 9:32-36. The permanent memory 31 is, for instance, “a PROM which is burned in during manufacture of the base unit.” *Id.*, 9:29-32.

Third, the base unit 12 applies H, K, N (previously generated by base unit 12), and R (same) to a cryptographic function and compares the result to the received authorization A. *Id.*, 9:50-63. If the result and authorization A match, then the authorization A is valid for the software package 17 on the base unit 12 for the number of uses N. *Id.*, 14-26; EX1003, ¶72.

Fourth, if the authorization A is valid, the base unit 12 updates the count of authorized uses at an address location defined by hash H in a non-volatile memory 37. *Id.*, 9:64-10:13. The non-volatile memory 37 can be, for example, “an EEPROM or a CMOS memory with battery backup.” *Id.*, 10:1-4.

When the user tries to use software package 17, the hash H is again generated, which is used to look up the number of remaining authorized uses, M, from the non-volatile memory 37. *Id.*, 10:33-43. If the number of remaining uses is greater than zero, then the software package 17 is permitted to run. *Id.*, 10:44-49. Hellman explained an alternative embodiment, where a specific number of uses is not maintained, but rather an unlimited number of uses is licensed. *Id.*, 10:55-65.

In other words, Hellman's disclosure could be used to license the software outright (*i.e.*, fully licensed instead of a number-of-uses license). EX1003, ¶76.

2. Overview of Chou

Chou addressed a problem of computer security: discouraging computer theft. EX1005, Chou, Abstract. Chou disclosed a modification to a personal computer that would render the computer inoperable unless a password stored in the BIOS memory is entered by the user or provided by an attached hardware device. *Id.*, Abstract, 1:5-8. The technique is implemented with a security routine stored in the BIOS memory. *Id.*, 2:10-32. Chou disclosed that the password stored in the BIOS memory could be updated by the user by using the security routine stored in the BIOS memory. *Id.*, 7:14-35, 8:42-9:50.

Chou made an important observation relevant to BIOS memory. Chou noted that “[m]any computer manufacturers have implemented password protection in the computer BIOS (Basic Input/Output System) which is integral to the operation of a personal computer.” *Id.*, 1:54-57. But when BIOS was stored in CMOS RAM, the security function could be bypassed by removing the power to the CMOS RAM. *Id.*, 1:57-62.

Chou went on:

Recent changes in the computer BIOS memory storage devices permit writing data to the BIOS memory, offering the opportunity to provide password protection within the same memory which stores the BIOS

routines. Thus, any attempt to delete protection will result in the BIOS routine being disabled, disabling the boot up process.

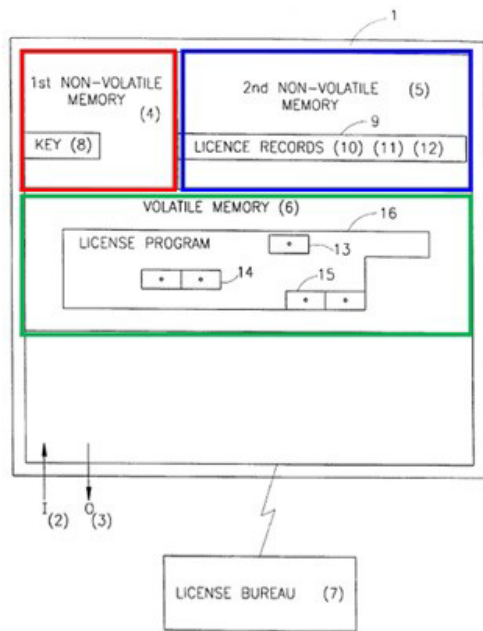
EEPROM flash devices may be programmed with BIOS routines which permit the user to enter data without requiring the computer to be returned to the manufacture. The present invention makes use of these new BIOS memory devices for effecting security measures which discourage theft.

Id., 1:63-2:7.

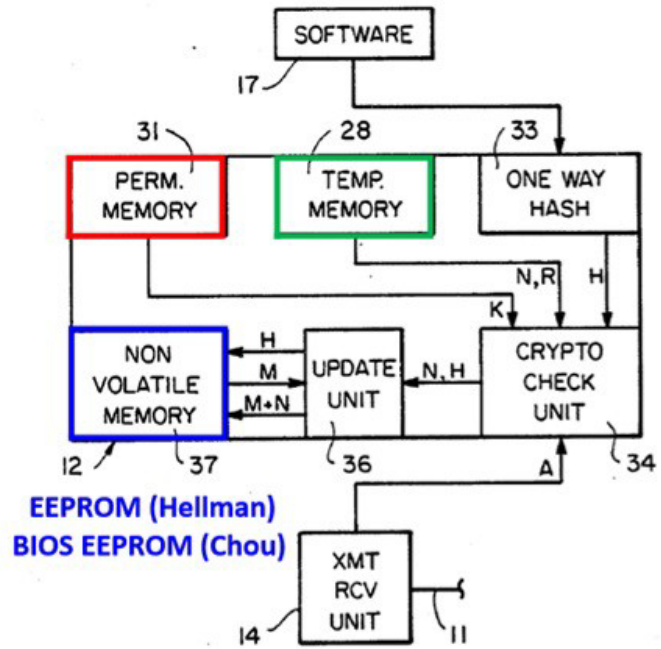
3. Motivations to Combine Hellman and Chou

As demonstrated in the analysis of the claims below, Hellman discloses almost all of the features of claim 1, including authorizing a software use through verification data stored in a non-volatile memory such as EEPROM. While Hellman does not explicitly disclose that the computer (base unit 12) has a BIOS and that nonvolatile memory 37 (*e.g.*, EEPROM) would be used to store the BIOS for the computer, a POSA would have found it obvious to provide a BIOS in the computer (base unit 12) and to store the BIOS in the nonvolatile memory 37 (*e.g.*, EEPROM), as disclosed by Chou. A POSA would have been motivated to make this modification for at least four independent reasons, as now discussed.

The combination of Hellman and Chou is visualized below, as compared against the '941 Patent.



EX1001, FIG. 1 (annotated).



EX1004, FIG. 6 (annotated).

First, Hellman disclosed as early as 1983 that a computer could store a number of licensed uses of a software program (the claimed “license record”) in an EEPROM memory. EX1004, 9:64-10:4; EX1003, ¶¶104, 134-137. While Hellman did not explicitly disclose that the computer used BIOS, or that the non-volatile memory 37 (*e.g.*, EEPROM) was the memory where the BIOS was stored, by the priority date of May 1998, it was well-known to a POSA that a computer would have BIOS and that it would be common to store it in EEPROM memory. EX1005, 1:54-62, 2:2-7, 3:21-35; EX1003, ¶¶105-111. *See also* ’941 File Wrapper, Office Action Response, dated Feb. 5, 2002, p. 7 (“Since all computers must have a BIOS ...”).

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

When applying Hellman's disclosure to a computer of the late 1990s, Hellman's disclosure would be applied on a computer with BIOS and a memory storing the BIOS. EX1003, ¶¶105-111. Thus, if a BIOS was not already present, a POSA would have been motivated to add a BIOS stored in a memory of the computer (base unit 12) of Hellman, at least because that was the standard—nearly universal—way in which computers operated prior to the priority date of the '941 Patent. *Id.*

A POSA would have been motivated to use the non-volatile memory 37 (*e.g.*, EEPROM) of Hellman to store the BIOS for Hellman's computer (base unit 12), in addition to the license information explicitly disclosed in Hellman, in order to achieve Hellman's purpose of discouraging tampering with the license information. EX1004, 4:22-26; EX1003, ¶¶112-116. Namely, when Hellman's technique was implemented on a computer of the late-1990s that required a BIOS, a POSA would have recognized that one such EEPROM that already existed in the computer would be the EEPROM used to store the BIOS, and that other information, like security routines should be stored in the **same** memory as the BIOS to prevent tampering by a user, as disclosed by Chou. EX1005, 3:21-35, 3:52-62; EX1003, ¶¶112-116. Thus, a POSA would have been motivated to use the non-volatile memory 37 (*e.g.*, EEPROM) from Hellman for storing the BIOS, as well as license information described in Hellman, because a POSA would have

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

recognized non-volatile memory 37 (*e.g.*, EEPROM) as an appropriate type of memory module for BIOS and one that would help prevent tampering with the license information. EX1005, 3:21-35, 3:52-62; EX1003, ¶¶112-116; *see also Sony Mobile Commc'ns AB v. Ancora Techs., Inc.*, IPR2021-00663, Paper 17 at 26 (P.T.A.B. June 10, 2021) (“Sony Institution Decision”) (rejecting Patent Owner’s argument that it would not have been obvious to modify Hellman to include BIOS memory). Moreover, it was common practice to store more than one thing in a single memory module in a computer. EX1003, ¶¶112-116, 119-120.

Second, a POSA would further have been motivated to use the non-volatile memory 37 in Hellman as the BIOS EEPROM of Chou because that would have been one of a limited number of design choices. EX1003, ¶114. Namely, a POSA would have recognized that in many computers of the era in the late 1990s, there would be few if any other EEPROM memory modules present on the computer other than the EEPROM storing the BIOS. *Id.* EEPROM was a specialized memory module, and it was not common to have more than one such modules in any computer. *Id.* Hence, the EEPROM storing the BIOS would have been one of at most a handful of available EEPROM storage modules with which the non-volatile memory 37 of Hellman could be implemented. *Id.* In many computers, the BIOS EEPROM would be the only EEPROM module in the computer. *Id.*

Third, a POSA would further have been motivated to use the non-volatile

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

memory 37 in Hellman as the BIOS memory of Chou because Chou disclosed that embedding sensitive information in the BIOS memory reduced the risk of tampering with that information. EX1003, ¶115. Chou explained that, by storing sensitive information (passwords in Chou) in the BIOS memory, any attempt to delete or disable the sensitive information would also disable the BIOS program. EX1005, 1:63-2:1; EX1003, ¶115. In other words, a user attempting to alter the sensitive information would be risking disabling the device entirely. EX1003, ¶115. A POSA would have recognized that this heightened risk would have discouraged tampering, thus making the BIOS memory a more secure place to store the license information from Hellman. *Id.*

Fourth, a POSA would further have been motivated to use the non-volatile memory 37 in Hellman as the BIOS EEPROM of Chou because that would have provided economic and operational efficiencies. EX1003, ¶116. Namely, using an EEPROM module other than non-volatile memory 37 to store the BIOS would have increased the cost of the computer and increased the space used on the motherboard for the chips. *Id.* Computer manufacturers generally sought to reduce the cost of parts in computers and to reduce the usage of board space where possible. *Id.* Because a single EEPROM module would have had sufficient space to store both the BIOS and other ancillary information, like the license information from Hellman, a POSA would have been motivated to use only a single EEPROM

module for both elements of information. *Id.*

Finally, because Chou discloses customizations of BIOS EEPROM with cryptographic values for add-on features, a POSA would have a reasonable expectation that such a use of the BIOS EEPROM as the non-volatile memory 37 would be successful. EX1003, ¶¶117-120. A POSA would not have been discouraged by any alleged incompatibility between Hellman and Chou from making the above-described combination. Wolfe Decl. ¶¶120A–120F; *see also* Sony Institution Decision at 26 (rejecting Ancora’s argument that Hellman and Chou are incompatible and cannot be combined).

4. Claim 1 preamble: “A method of restricting software operation within a license for use with a computer including an erasable, non-volatile memory area of a BIOS of the computer, and a volatile memory area; the method comprising the steps of:”

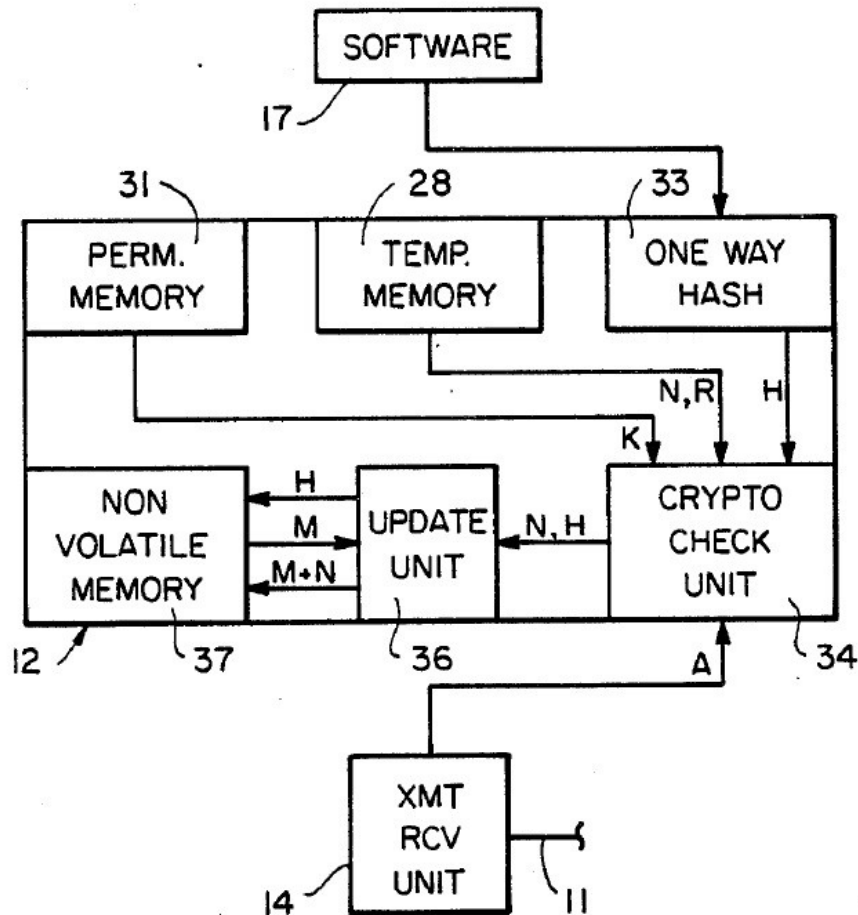
Even if the preamble is considered limiting, Hellman disclose all aspects of the preamble of claim 1, other than explicit mention of a BIOS and a memory storing the BIOS. These remaining features would have been obvious based on knowledge in the art and as demonstrated by Chou.

Hellman disclosed the required “method of restricting software operation within a license” in the form of its method of limiting use of software within authorized uses. EX1004, 9:29-10:13, 10:33-54, 10:55-65; EX1003, ¶¶98-104.

Hellman disclosed that the method is for use with the claimed “computer” in

the form of base unit 12. EX1004, FIGs. 1, 6; *see also id.*, 2:24-27 (describing “acquaintances with similar base units (computers)”); EX1003, ¶¶98-104.

Hellman disclosed that the computer (base unit 12) includes the claimed “erasable, non-volatile memory area of a BIOS of the computer, and a volatile memory area.” For example, the base unit 12 has the claimed “volatile memory area” in the form of temporary memory 28, *e.g.*, RAM (Random Access Memory). EX1004, FIG. 6; *see also id.*, 8:67-68 (“Base unit 12 stores these values in a temporary memory 28, for example a RAM ... [.]”); EX1003, ¶¶98-104. The base unit 12 includes the claimed “erasable, non-volatile memory area” in the form of non-volatile memory 37, which could be implemented as EEPROM. EX1004, FIG. 6; *see also id.*, 10:1-4; EX1003, ¶¶98-104.



EX1004, FIG. 6.

Hellman did not explicitly disclose that the computer (base unit 12) had BIOS stored in memory. As a result, Hellman did not explicitly disclose that the non-volatile memory 37 (*e.g.*, EEPROM) is the claimed “erasable, non-volatile memory area of a BIOS of the computer.” But Chou disclosed this feature in the form of BIOS EEPROM 15, and a POSA would have understood that EEPROM, which stood for electrically erasable programmable read only memory, was a type of erasable, non-volatile memory. EX1005, FIGs. 1, 3, 7; 1:54-2:7; 3:21-35; EX1003, ¶¶104-106. For the reasons described with respect to the motivation to

combine, a POSA would have found it obvious to implement Hellman on a computer in which the **same** erasable, non-volatile memory 37 (*e.g.*, EEPROM) stored both the license information disclosed in Hellman and the BIOS, such as disclosed by Chou. *See supra* § VII.A.3; *see also* EX1005, 1:63-2:7.

5. Claim 1.a: “selecting a program residing in the volatile memory,”

Hellman discloses this element in the form of selecting software package 17 (the required “program”), which, when the software package 17 is a computer program, would reside in temporary memory 28, such as RAM (the required “volatile memory”). POSA would have recognized that, at least when software package 17 was a computer program and software player 42 was a CPU, the software package 17 would be present in volatile memory, such as temporary memory 28 (“for example RAM,” EX1004, 8:67-9:2), during any one of numerous times that the software package 17 was selected. EX1003, ¶¶121-129.

Hellman disclosed numerous selections of the software package 17. Hellman disclosed that the software package 17 is obtained “by purchasing it at a store, over telephone line, or in some similar manner.” EX1004, 5:51-56; EX1003, ¶¶123-127. Hellman disclosed selecting the software package 17 as part of generating a request for authorization, such as by extracting the software name from the software package 17. EX1004, 5:57-61; EX1003, ¶¶123-127.

Hellman disclosed selecting the software package 17 for input to the

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

cryptographic hash function to calculate the cryptographic hash H. EX1004, 9:15-28; EX1003, ¶¶123-127. Hellman disclosed selecting the software package 17 for use by the software player 42. EX1004, 10:33-65; EX1003, ¶¶123-127. If the software package 17 “is a computer program, then software player 42 would be a microprocessor or central processing unit (CPU).” EX1004, 10:66-11:3; EX1003, ¶¶123-127.

A POSA would have recognized that, at least when software package 17 was a computer program and software player 42 was a CPU, the software package 17 would be present in volatile memory, such as temporary memory 28 (“for example RAM,” EX1004, 8:67-9:2), during one of the selections identified above. EX1003, ¶¶123-129. For example, a POSA would have recognized that the software package 17 would be in RAM 28 when the software package 17 was applied to one way function generator 33 for generation of hash value H. EX1004, 9:16-28; EX1003, ¶¶123-129. As a further example, a POSA would have found it obvious to be running the software package 17 in RAM 28 when attempting to operate software package 17 on CPU (software player) 42. EX1004, 10:66-11:3; EX1003, ¶¶123-129.

Furthermore, a POSA would have found it obvious to modify Hellman to have the software package 17 residing in the temporary memory 28 while it was selected. For example, a POSA would have found it obvious to maintain the

software package 17 in temporary memory 28 after selection of the software name, 5:57-61, and until selection for input to the cryptographic hash function, EX1004, 9:15-28. Namely, a POSA would have been motivated to maintain the software package 17 in temporary memory 28 while awaiting the authorization A because a POSA would have recognized that this would have avoided unnecessarily writing software package 17 to some other memory location and then having to re-read it. EX1003, ¶¶128-129.

6. Claim 1.b: “using an agent to set up a verification structure in the erasable, non-volatile memory of the BIOS, the verification structure accommodating data that includes at least one license record,”

Hellman discloses this element because it disclosed using update unit 36 (acting as the required “agent”) to set up a verification structure in non-volatile memory 37 (the required “erasable, non-volatile memory”) as the non-volatile memory 37 was preferably implemented as EEPROM, EX1004, 10:1-4, which was an erasable, non-volatile memory. EX1003, ¶¶133-138. For the reasons described with respect to the motivation to combine, a POSA would have found it obvious to implement non-volatile memory 37 (*e.g.*, EEPROM) from Hellman as the same EEPROM that also stores BIOS, such as disclosed by Chou. *See supra* § VII.A.3.

The update unit 36 sets up the required “verification structure” in the non-volatile memory 37 at least in the form of storing the value M at a specific address H for a software program identified by that hash value H. EX1003, ¶¶133-138. The

value M is the required “license record”, because it indicates the scope of authorized use—the number of uses, where “M” is the number—for the specific software package 17 identified by hash value H. *Id.* Storing the value M at the address H constitutes setting up a verification structure because it includes storing a license record at a specific license record location that corresponds to the licensed program. *See* EX1001, 1:59-62; 6:17-21; EX1003, ¶¶133-138.

In addition, Dr. Wolfe explained that the authorization and billing unit 13 may cooperate with the update unit 36 to act as the “agent” because “the update unit 36 would have been implemented by a software routine, potentially along with a hardware module.” EX1003, ¶137. A POSA would have recognized that the update unit 36 and the authorization and billing unit 13 were both implemented in software or a combination of software and hardware. EX1003, ¶¶137-138A; *see also* Sony Institution Decision at 27–29 (noting with approval Dr. Wolfe’s opinion that Hellman’s “agent” includes a combination of software and hardware).

7. Claim 1.c: “verifying the program using at least the verification structure from the erasable non-volatile memory of the BIOS, and”

Hellman disclosed this element because it disclosed using the value M (the required “license record”) that is stored in the non-volatile memory 37 to verify software package 17 (the required “program”). Hellman disclosed that when an

attempt is made to run software package 17, the value H is generated and sent to the update unit 36. EX1004, 10:33-43; EX1003, ¶¶151-152. The update unit 36 uses H as an address in the non-volatile memory 37 to verify if a license exists for the software package 37. EX1004, 10:33-43; EX1003, ¶¶151-152. If a license does exist for the software package 17 in the non-volatile memory 37, then the update unit 36 retrieves the number of remaining authorized uses M. EX1004, 10:44-54; EX1003, ¶¶151-152. A determination is made as to whether the number of authorized uses is greater than zero. EX1004, 10:44-54; EX1003, ¶¶151-152. Thus Hellman discloses verifying both that the software package 17 is licensed, and that at least one authorized use remains on the license.

8. Claim 1.d: “acting on the program according to the verification.”

Hellman disclosed this element, because it discloses allowing the software package 17 to be used if a license record was found in the non-volatile memory 37 and there are authorized uses remaining. EX1004, 10:40-49; EX1003, ¶¶154-155.

9. Claim 2: “A method according to claim 1, further comprising the steps of: establishing a license authentication bureau.”

Hellman disclosed this element because it discloses establishing the authorization and billing unit 13. Hellman discloses an implementation of the authorization and billing unit 13 that creates an authorization A in order to securely pass license information to the base unit 12. EX1004, 6:16-7:16; EX1003, ¶¶156-

158. Hellman also describes authorization A as “an authenticator which is a cryptographic function of the base unit’s key, the software, the number of times use of the software is authorized, and the random number generated by the base unit.” EX1004, 4:51-55; EX1003, ¶¶156-158.

Hence, the authorization and billing unit 13 is the required “license authentication bureau” at least because it generates a data structure that authenticates license information transmitted to the base unit 12. EX1003, ¶¶156-158.

10. Claim 11: “A method according to claim 1 wherein the volatile memory is a RAM.”

Hellman disclosed this limitation, because it disclosed temporary memory 28 is “for example a RAM,” and a POSA would have understood that RAM is volatile memory. EX1004, 8:67-68; EX1003, ¶221.

11. Claim 13: “The method of claim 1, wherein a unique key is stored in a first non-volatile memory area of the computer.”

Hellman discloses this limitation, because it discloses storing a serial number and a key, K, (the required “unique key”) in the permanent memory 31, for example a PROM, (the required “first non-volatile memory area”) of the base unit 12 (the required “computer”). EX1004, 8:61-9:15, 9:29-32; EX1003, ¶¶229-231. A POSA would have understood that PROM stands for programmable read only memory, and that permanent memory 31, and specifically a PROM, is a type of

non-volatile memory. EX1003, ¶¶229-231.

B. Ground II: Claims 1-3, 6-14, and 16 were obvious over the combined teachings of Hellman, Chou, and Schneck.

1. Overview of Schneck

Schneck disclosed a technique that “controls access to and use and distribution of data.” EX1006, 6:49-50. “[W]hen the data represents a computer software program, this invention can control how much of the software’s functionality is available.” *Id.*, 6:53-56. Similar to Hellman and the ’941 Patent, Schneck seeks to prevent the authorization to use software on one device from being used on another, unauthorized device, which Schneck calls the “secondary distribution” problem. *Id.*, 6:57-62; *see also id.*, 2:40-67.

While Schneck discloses a secure hardware module, access mechanism 114, for preventing unauthorized secondary distribution, Schneck also discloses other more fundamental features relevant to the claims of the ’941 Patent. For example, Schneck discloses that “[i]n general, within the system, the data are encrypted on any non-volatile storage devices so that they remain unavailable in the case of tampering.” *Id.*, 17:6-12. “Since all storage of data on internal non-volatile memory devices (for example, disks, flash memory, and the like) is encrypted, this ensures that a physical attack on the system will not result in compromise of plaintext.” *Id.*, 25:64-67. Among other information that can be encrypted are access rules that are used to control how a user can access the protected data. *Id.*,

9:50-54, 10:35-42, 15:20-29.

2. Motivations to Combine Hellman, Chou, and Schneck

Hellman disclosed most of the features of claim 1, and Hellman in combination with Chou disclosed all of the features of claim 1. Schneck contains teachings relevant to various dependent claims. For example, based on the teachings of Schneck, a POSA would have found it obvious to store the value M in Hellman (the required “license record”) in *encrypted* form in the non-volatile memory 37 in Hellman, which a POSA would have found obvious to also store the BIOS, as discussed with respect to the motivations to combine Hellman and Chou, *see supra* § VII.A.3.

Hellman and Schneck both attempt to solve the problem of “copy protection” or “secondary distribution,” *i.e.*, an authorized user distributing unauthorized copies of licensed software. EX1004, 1:39-2:53; EX1006, 2:40-67; EX1003, ¶¶139-140.

Hellman addressed part of this problem. Hellman’s system prevents malicious duplication of the authorization signal if it is intercepted on the insecure communication channels between the computer and the authorizing entity. EX1004, 6:62-7:16; EX1003, ¶¶141-143. This is the case because the authorization A is encrypted with a key specific to the base unit 12 (the required “computer”) and a cryptographic hash specific to the software package 17 (the required

“program”). EX1004, 6:62-7:16; EX1003, ¶¶141-143. Thus, a malicious actor could not reuse the authorization A on another computer or for another software package. EX1003, ¶¶141-143.

However, a POSA would have recognized that with Hellman’s system, the number of authorized uses, M, stored in non-volatile memory 37 could be changed (i.e., increased) by a malicious actor. *Id.* This is the case because M is stored in plaintext at an address location determined by hash value H. EX1004, 9:64-10:13; EX1003, ¶¶141-143. Further, in the embodiments of Hellman where M is a default value representing “unlimited number of uses of a software package,” Hellman, 10:55-65, a malicious actor would be able to store this same default value for M at the address location in non-volatile memory 37 for any other software package, thereby obtaining access to other software packages without an appropriate license. EX1003, ¶¶141-143. In fact, this same default value for M could be stored in the non-volatile memory 37 of another base unit, thus allowing for unauthorized secondary distribution. *Id.*

A POSA would have found it obvious to address this shortcoming of Hellman based on the teachings of Schneck. Schneck disclosed that licensing information is transmitted in encrypted form. EX1006, 9:46-59 (“The packaged data 108 may include access rules 116 in encrypted form[.]”); EX1003, ¶¶144-150.

Schneck also disclosed that any information stored on a non-volatile

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

memory, as done in Hellman, should be stored in encrypted form to prevent an unauthorized use of a licensed software. EX1006, 25:64-67 (“Since all storage of data on internal non-volatile memory devices (for example, disks, flash memory, and the like) is encrypted, this ensures that a physical attack on the system will not result in compromise of plaintext.”); EX1003, ¶¶144-150. Schneck explained that this prevents “secondary distribution” of a licensed program, an issue inherent with unencrypted data as seen in Hellman. EX1006, 25:49-62; EX1003, ¶¶144-150.

Based on Schneck’s disclosure, a POSA would have found it obvious to store the licensing information in non-volatile memory 37 in encrypted form to address Hellman’s deficiencies. EX1003, ¶¶144-150. For example, a POSA would have found it obvious to store authorization A—which included M as a component value—at memory address H in non-volatile memory 37, instead of storing plaintext value M. *Id.* A POSA would have found this especially useful where M was the default value representing “unlimited number of uses of a software package,” EX1004, 10:55-65, given that M would not need to be incremented or decremented. EX1003, ¶¶144-150. A POSA would have recognized that this modification of Hellman would have prevented a malicious actor from using the license authorization for another software package on the same base unit (because authorization A is encrypted with hash value H for the software package 17), and would have prevented a malicious actor from using the license authorization on

another base unit (because authorization A is encrypted with a key SK unique to the base unit). EX1003, ¶¶144-150.

A POSA would have been motivated to modify Hellman in this way because Hellman and Schneck both attempted to prevent unauthorized secondary distribution, while Schneck removed a shortcoming in that regard in the system of Hellman. EX1004, 1:39-2:53; EX1006, 2:40-67; EX1003, ¶¶144-150. Namely, a POSA would have recognized based on the teachings of Schneck that storing the required “license record” in encrypted form in the non-volatile memory 37 of Hellman would have furthered Hellman’s goal of preventing a license authorization from being improperly duplicated. EX1006, 17:6-12, 25:64-67; EX1003, ¶¶144-150. Because Hellman already disclosed an encrypted license record in the form of authorization A, a POSA would have had a reasonable expectation of success in modifying Hellman to store the authorization A. EX1003, ¶¶144-150.

Various other modification to Hellman that would have been obvious to a POSA based on the disclosures of Schneck are discussed below.

3. **Claim 1. preamble: “A method of restricting software operation within a license for use with a computer including an erasable, non-volatile memory area of a BIOS of the computer, and a volatile memory area; the method comprising the steps of:”**

Even if the preamble is limiting, a POSA would have found the limitations

of the preamble obvious based on the combination of Hellman and Chou. Hellman disclosed a computer (base unit 12) with a volatile memory area (temporary memory 28) and a non-volatile memory area (non-volatile memory 37). *See supra* § VII.A.4. Hellman disclosed a method of restricting software operation (software package 17) within a license (authorized uses M). *Id.* A POSA would have found it obvious to modify Hellman's system to provide the non-volatile memory area (non-volatile memory 28) as the non-volatile memory storing the BIOS of the computer, a commonly known technique at the priority date, as exemplified by Chou. *Id.*

4. Claim 1.a: “selecting a program residing in the volatile memory,”

A POSA would have found it obvious based on the teachings of Hellman to select a software package 17 (the required “program”) residing in temporary memory 28 (the required “volatile memory”). *See supra* § VII.A.5. Schneck further demonstrates that a POSA would have recognized that a first step to accessing protected information would be to “request the operating system to read such data into memory.” EX1006, 18:7-10; EX1003, ¶¶130. Once in memory, the protected information, such as software package 17 from Hellman, would be selected from the temporary memory 28, such as: for extracting the software name, EX1004, 5:57-61, for input to the cryptographic hash function, EX1004, 9:15-28; or for use by the software player 42, EX1004, 10:33-65. EX1003, ¶¶130-132. Thus, while it

was readily obvious for a POSA to select a program residing in the volatile memory, this feature would have been further obvious based on the teachings of Schneck.

5. Claim 1.b: “using an agent to set up a verification structure in the erasable, non-volatile memory of the BIOS, the verification structure accommodating data that includes at least one license record,”

A POSA would have found it obvious based on the disclosures of Hellman and Chou to use an agent (update unit 36) to set up a verification structure (memory location in non-volatile memory 37 as defined by hash value H) in the erasable, non-volatile memory of the BIOS (non-volatile memory 37 provided as EEPROM, storing BIOS as taught by Chou), with the verification structure accommodating data that includes at least one license record (authorized uses value M). *See supra* § VII.A.6.

Further, a POSA would have found it obvious based on the teachings of Schneck to modify Hellman to store an *encrypted* license record (authorization A). *See supra* § VII.B.2. Namely, a POSA would have found it obvious to store the authorization A in the non-volatile memory 37, in place of the plaintext value M. EX1003, ¶¶139-150. Hellman already disclosed that the authorization A is transmitted to the base unit 12. EX1004, 6:9-15; EX1003, ¶65. While Hellman disclosed generating a local copy of the authorization A and then only storing the component value M in non-volatile memory 37, EX1004, 9:50-10:13, a POSA

would have recognized that the authorization A could itself be stored in the non-volatile memory 37, *see supra* § VII.B.2, EX1003, ¶¶169-172, 144-150.

A POSA would have been especially motivated to store the authorization A instead of the hash value H when an “unlimited number of uses” was licensed. EX1004, 10:50-54; EX1003, ¶148. First, because the “unlimited license” value could be duplicated for any other software package, a POSA would have recognized that it would have been especially important to protect that default value in encrypted form in the non-volatile memory 37. EX1003, ¶148.

Second, because the “unlimited license” value would not need to be decremented when the software package 17 was used, EX1004, 10:62-65, a POSA would have recognized that encrypted authorization A could be conveniently stored in non-volatile memory 37 because it would not need to be modified each time the software package 17 was used. EX1003, ¶148.

Additionally, a POSA would have been motivated to store the authorization A in the non-volatile memory 37 instead of the plaintext value M because this would have been the exchange of one well-known encryption/decryption timing scheme for another. EX1003, ¶¶139-150. In particular, a POSA would have recognized that the authorization A could be verified a single time, as Hellman discloses, or verified each time the software package 17 was used. EX1003, ¶153. Single-instance verification and as-needed verification were both well-known

schemes in the art, and thus a POSA would have been motivated to use modify Hellman's system to use the latter as a matter of exchanging one well-known approach for another well-known approach amongst a finite set of possible approaches. EX1003, ¶¶139-150.

6. Claim 1.c: “verifying the program using at least the verification structure from the erasable non-volatile memory of the BIOS, and”

Hellman disclosed this element in the form of verifying the software package 17 (the required “program”) using the value stored in non-volatile memory 37 at the memory address identified by hash value H (the required “verification structure”) whenever the software package 17 was used. *See supra* § VII.A.7; *see also* EX1004, 10:33-43, 10:55-65; EX1003, ¶¶151-152.

When Hellman was modified based on the teachings of Schneck to store the authorization A in the non-volatile memory 37, *see supra* § VII.B.5, a POSA would have recognized that Hellman's verification would have been performed using the stored authorization A. EX1003, ¶153. For example, a POSA would have recognized that the authorization A could have been decrypted using the key K stored in permanent memory 31. EX1004, 9:29-40; EX1003, ¶153. The retrieved value M could then be verified to determine that, e.g., the value matched the “unlimited license” value for the software package 17. EX1004, 10:55-65; EX1003, ¶153.

7. Claim 1.d: “acting on the program according to the verification.”

Hellman disclosed this element, because it disclosed allowing the software package 17 (the required “program”) to be used if a license record was found in the non-volatile memory 37 and there were authorized uses remaining. EX1004, 10:40-49; EX1003, ¶¶154-155.

8. Claim 2: “A method according to claim 1, further comprising the steps of: establishing a license authentication bureau.”

Hellman disclosed this element in the form of establishing the authorization and billing unit 13. *See supra* § VII.A.9.

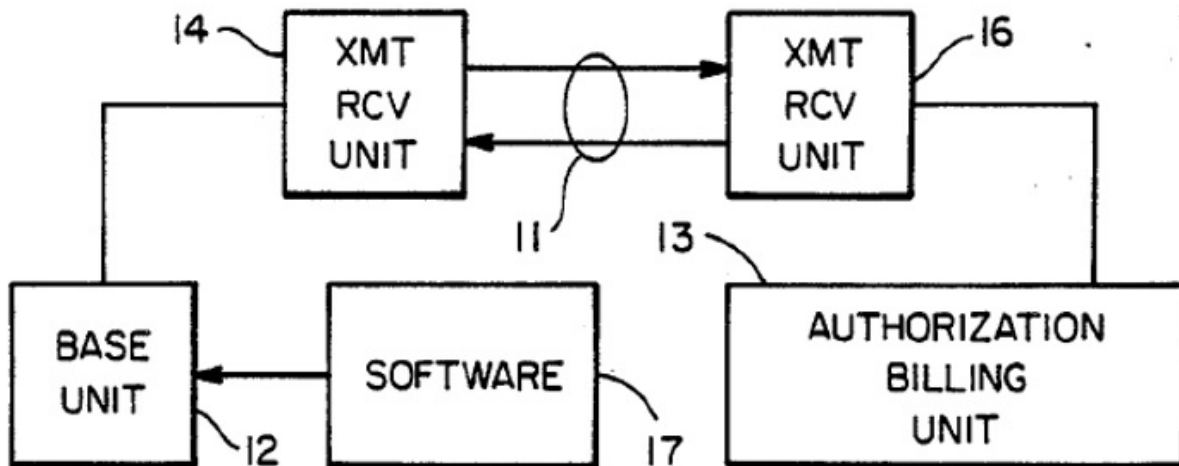
9. Claim 3 preamble: “A method according to claim 2, wherein setting up a verification structure further comprising the steps of:”

See discussion above of claim elements 1.b and 2. *See supra* §§ VII.B.5, VII.B.8.

10. Claim 3.a: “establishing, between the computer and the bureau, a two-way data-communications linkage;”

Hellman disclosed this element, because it disclosed establishing a two-way data communication between the base unit 12 (the required “computer”) and the authorization and billing unit 13 (the required “bureau”) over insecure communication channel 11 (the required “two-way data communications linkage”). EX1004, 5:39-6:8; EX1003, ¶¶160-162. In one direction, the base unit 12 communicates a request to the authorization and billing unit 13. EX1004, 5:57-63;

EX1003, ¶¶160-162. In the other direction, the authorization and billing unit 13 communicate an authorization A to the base unit 12. EX1004, 6:3-8; EX1003, ¶¶160-162. The channel 11 is illustrated below.



EX1004, FIG. 1.

11. **Claim 3.b: “transferring, from the computer to the bureau, a request-for-license including an identification of the computer and the license-record’s contents from the selected program;”**

Hellman disclosed this element, because it disclosed the base unit 12 (the required “computer”) transferring a “user originated request for software use” (the required “request-for-license”) to the authorization and billing unit 13 (the required “bureau”). EX1004, 5:57-61; EX1003, ¶¶163-172. The request includes the required “identification of the computer,” because it includes a serial number value, which is a “serial number, identification number, user name or similar identifier unique to base unit 12.” EX1004, 5:57-65; EX1003, ¶¶163-172.

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

The request also includes the required “license record’s contents form the selected program” because it includes the software name identifying the software, as well as other information like the number of additional uses, N. EX1004, 5:57-66; EX1003, ¶¶163-172.

Furthermore, a POSA would have recognized that the request could have included different and/or additional information.

First, a POSA would have recognized that the hash value H could have been included in the request in place of the software name. EX1003, ¶¶163-172. A POSA would have been motivated to use the hash value H to more precisely identify the software package 17 for which the user was requesting a license. *Id.*

For instance, in an implementation of the system of Hellman that supported multiple software manufacturers, and thus the software name may not have guaranteed unique identification of a software package, a POSA would have been motivated to include hash value H in the request instead of or in addition to the software name. *Id.* Hellman itself suggests that hash value H “can be used in place of SOFTWARE NAME to name the software being used.” EX1004, 9:66-10:1; EX1003, ¶¶163-172.

Second, a POSA would have recognized that the request could have used a public key for the base unit 12 as the “serial number, identification number, user name or similar identifier unique to base unit 12.” EX1004, 5:59-65; EX1003,

¶¶163-172. Hellman disclosed that the serial number could be any “identifier unique to base unit 12,” EX1004, 5:59-65, and Schneck disclosed that a public key could be used to identify a computer system, EX1006, 11:32-35. EX1003, ¶¶163-172. A POSA would have recognized that by the priority date of the ’941 Patent, a public key could be used as an identifier for a computer. EX1003, ¶¶163-172.

A POSA would have been motivated to use a public key as the identifier for the base unit 12 for numerous reasons. First, a POSA would have recognized that a public key was a well-known technique for identifying a device over a network connection. EX1003, ¶¶163-172. Second, a POSA would have recognized that the public key could have been used instead of the secret key SK to encrypt the authorization A at the authorization and billing unit 13. *Id.* This would have allowed the authorization and billing unit 13 to securely generate the authorization A without needing to maintain a lookup table for serial numbers or a local version of secret keys for base units. EX1004, 6:16-30; EX1003, ¶¶163-172. This would have both improved the security of Hellman’s system and simplified the implementation of the system. EX1003, ¶¶163-172.

In sum, a POSA would have found it obvious to include in the request from the base unit 12 the component values that ultimately make up the authorization A. *Id.* And because a POSA would have found it obvious to store the authorization A as the license record in the non-volatile memory 37, *see supra* §§ VII.B.5, the

request from the base unit 12 would have included the license record's contents.

12. Claim 3.c: “forming an encrypted license-record at the bureau by encrypting parts of the request-for-license using part of the identification as an encryption key;”

Hellman disclosed this element, because it disclosed the billing and authorization unit 13 (the required “bureau”) forming an encrypted license record in the form of authorization A. EX1004, 6:16-7:16; EX1003, ¶¶173-178. Namely, Hellman disclosed including the value N in the request, EX1004, 5:57-6:2, and encrypting at least value N as part of the encrypted license record, EX1004, 6:3-8, 6:62-7:2. EX1003, ¶¶173-178.

Furthermore, as discussed above, when Hellman was modified to include a public key in the request as an identification of the base unit 12, a POSA would have been motivated to use the public key to encrypt the authorization A. *see supra* §§ VII.B.11; EX1003, ¶¶173-178. Therefore, the license record would have been encrypted using part of the identification from the request as the encryption key. EX1003, ¶¶173-178.

13. Claim 3.d: “transferring, from the bureau to the computer, the encrypted license-record; and”

Hellman disclosed this element, because it disclosed the billing and authorization unit 13 (the required “bureau”) transferring the authorization A (the required “encrypted license-record”) to the base unit 12. EX1004, 6:3-15; EX1003, ¶¶179-180.

14. Claim 3.e: “storing the encrypted license record in the erasable non-volatile memory area of the BIOS.”

While Hellman disclosed storing the number of authorized uses M in the non-volatile memory 37, a POSA would have found it obvious to store the authorization A in the non-volatile memory A. *See supra* § VII.B.5.

15. Claim 6: “A method according to claim 1 wherein selecting a program includes the steps of: establishing a licensed-software-program in the volatile memory of the computer wherein said licensed-software-program includes contents used to form the license-record.”

A POSA would have found it obvious to load a licensed software program (software package 17) into volatile memory (temporary memory 28). *See supra* § VII.B.4. Hellman discloses that the licensed software program includes contents used to form the license record, because Hellman discloses that the software package 17 is itself used to generate the hash value H, which is part of the authorization A. EX1004, 6:27-35, 6:62-66, 9:16-28; EX1003, ¶¶185-188. And as discussed above, a POSA would have found it obvious to store the authorization A as the license record in the non-volatile memory 37. *See supra* § VII.B.5.

16. Claim 7 preamble: “A method according to claim 6 wherein using an agent to set up the verification structure includes the steps of:”

See discussion above of claim elements 1.b and 6. *See supra* §§ VII.B.5, VII.B.15.

17. Claim 7.a: “establishing or certifying the existence of a pseudo-unique key in a first non-volatile memory area of the computer; and”

Hellman disclosed this element, because it disclosed storing a serial number and a key, K, (the required “pseudo-unique key”) in the permanent memory 31 (the required “first non-volatile memory area”), which could be a non-volatile memory such as PROM. EX1004, 8:61-9:15, 9:29-32; EX1003, ¶¶190-196.

Furthermore, a POSA would have recognized that when Hellman was modified to store authorization A in the non-volatile memory 37, *see supra* § VII.B.5, the modified update unit 36 and/or other associated memory access modules would have been used to certify the existence of the key K in permanent memory 31 in order to be able to verify the authorization A contained valid information for the software package 17. EX1003, ¶¶190-196.

18. Claim 7.b: “establishing at least one license-record location in the first nonvolatile memory area or in the erasable, non-volatile memory area of the BIOS.”

Hellman disclosed this element, because it disclosed establishing a location at an address associated with hash value H (the required “license-record location”) in the non-volatile memory 17 (the required “erasable, non-volatile memory area of the BIOS”). EX1004, 9:64-10:12; EX1003, ¶¶197-200. As discussed above, a POSA would have found it obvious to implement the non-volatile memory 17 as the erasable, non-volatile memory area of the BIOS. *See supra* § VII.B.

19. Claim 8 preamble: “A method according to claim 6 wherein establishing a license-record includes the steps of:”

See discussion above of claim element 6. *See supra* § VII.B.15.

20. Claim 8.a: “forming a license-record by encrypting of the contents used to form a license-record with other predetermined data contents, using the key; and”

Hellman disclosed this element, because it disclosed forming authorization A (the required “license-record”) by encrypting the contents used to form the license record (*e.g.*, the hash value H) with “other predetermined data contents” (*e.g.*, values N and R), using the key, K (which can be the same as key SK).

EX1004, 6:62-7:16, 9:32-36; EX1003, ¶¶202-206. The result of this encryption is the authorization A, which is a license record at least because it indicates the right to operate the software package 17 on the base unit 12. EX1004, 6:3-15, 7:3-16; EX1003, ¶¶202-206. As discussed above, a POSA would have found it obvious to store the authorization A as the license record in the non-volatile memory 17. *See supra* § VII.B.5.

21. Claim 8.b: “establishing the encrypted license-record in one of the at least one established license-record locations.”

Hellman disclosed storing a license record at a license-record location in the form of storing a number of authorized uses M at an address associated with hash value H in the non-volatile memory 17. EX1004, 9:64-10:13; EX1003, ¶¶207-209. As discussed above, a POSA would have found it obvious to store the authorization A instead of the plaintext value M as the license record in the non-

volatile memory 17. *See supra* § VII.B.5.

22. Claim 9 preamble: “A method according to claim 7 wherein verifying the program includes the steps of:”

See discussion above of claim elements 1.c and 7. *See supra* §§ VII.B.6, VII.B.16.

23. Claim 9.a: “encrypting the licensed-software-program's license-record contents from the volatile memory area or decrypting the license-record in the erasable, non-volatile memory area of the BIOS, using the pseudo-unique key; and”

Hellman disclosed verifying the plaintext value M stored in the non-volatile memory 37 when the user attempts to use the software package 17. EX1004, 10:33-65; EX1003, ¶¶210-212. As discussed above, a POSA would have found it obvious to store the authorization A instead of the plaintext value M as the license record in the non-volatile memory 17. *See supra* § VII.B.5. A POSA would have recognized that with this modification, when the user attempts to use the software package 17, the encrypted license record (authorization A) in the non-volatile memory are of the BIOS (non-volatile memory 37) would be decrypted in order to retrieve the value M. EX1003, ¶¶210-212. And because the authorization A was encrypted using the key K, the key K would be used to decrypt the authorization A. EX1004, 6:62-7:2, 9:32-36; EX1003, ¶¶210-212.

- 24. Claim 9.b: “comparing the encrypted licenses-software-program’s license-record contents with the encrypted license-record in the erasable, non-volatile memory area of the BIOS, or comparing the license-software-program's license-record contents with the decrypted license-record in erasable non-volatile memory area of the BIOS.”**

A POSA would have found it obvious to store the authorization A instead of the plaintext value M as the license record in the non-volatile memory 17. *See supra* § VII.B.5. One reason for doing so would be to prevent a user from copying the license record for one software package 17 and using it for another software package 17 on the same base unit 12. *Id.*; EX1003, ¶¶213-217. This would have prevented unauthorized uses of the second software package 17. *See supra* § VII.B.5; EX1003, ¶¶213-217.

However, a POSA would have recognized that this security benefit would only have been realized if, after decrypting the authorization A, the component hash value H was compared to the hash value H for the software package 17 currently being used. EX1003, ¶¶213-217. As such, a POSA would have found it obvious to compare the decrypted license record with the license record contents of the software package 17, i.e., the hash value H generated for the software package 17. EX1004 9:66-10:1; EX1003, ¶¶213-217.

- 25. Claim 10: “A method according to claim 9 wherein acting on the program includes the step: restricting the program's operation with predetermined limitations if the comparing yields non-unity or insufficiency.”**

Hellman disclosed this limitation, because it discloses restricting the software package 17 from being used if there is no license record found in the non-volatile memory 37 or there are no authorized uses left. EX1004, 10:40-54; EX1003, ¶¶218-220.

A POSA would have found it obvious to compare the hash value H from the authorization A with the hash value H for the software package 17 currently being used. *See supra* § VII.B.24. A POSA would have recognized that if this comparison yielded non-unity, that is, if the hash values do not match, then the authorization A did not correspond to the software package 17 currently being used. EX1003, ¶¶218-220. A POSA would have found it obvious to prevent the user from using the software package in this case, in order to prevent unauthorized use of the software package 17. *Id.*

- 26. Claim 11: “A method according to claim 1 wherein the volatile memory is a RAM.”**

Hellman disclosed this limitation because it discloses that the temporary memory 28 (the required “volatile memory”) is “for example a RAM.” *See supra* § VII.A.10.

27. Claim 12: “The method of claim 1, wherein a pseudo-unique key is stored in the non-volatile memory of the BIOS.”

A POSA would have found it obvious to store the authorization A instead of the plaintext value M as the license record in the non-volatile memory 17. *See supra* § VII.B.5. A POSA would have recognized that with this modification, a pseudo-unique key in the form of hash value H would be stored in the non-volatile memory of the BIOS (non-volatile memory 17) as a component of the authorization A. EX1004, 6:31-61; EX1003, ¶¶222-228.

In addition, a POSA would have found it obvious to use a public key architecture in the system of Hellman. *See supra* § VII.B.11. When modified to use a public key architecture, a POSA would have recognized that the public key could be stored in the non-volatile memory 37. EX1003, ¶¶222.

A POSA would have been motivated to store the public key in the non-volatile memory 37 because that would be one of a limited number of design choices, i.e., there were a limited number of memory modules in which to store the public key. EX1004, 8:61-9:15; EX1003, ¶¶222-228. Furthermore, a POSA would have recognized that the public key would not need to be stored in the PROM like the secret key K, because the public key was designed to be shared outside the base unit 12. EX1004, 9:29-32; EX1006, 11:31-35; EX1003, ¶¶222-228. Thus for this additional reason, a POSA would have found it obvious to store a pseudo-unique

key in the non-volatile memory 37.

- 28. Claim 13: “The method of claim 1, wherein a unique key is stored in a first non-volatile memory area of the computer.”**

Hellman disclosed this limitation because it disclosed storing a serial number and a key, K, in the permanent memory 31, which could be a non-volatile memory such as PROM. *See supra* § VII.A.11.

- 29. Claim 14: “The method according claim 13, wherein the step of using the agent to set up the verification record, including the license record, includes encrypting a license record data in the program using at least the unique key.”**

Hellman disclosed this limitation because it disclosed encrypting license record data in the program (*e.g.*, the value H generated from software package 17) using the key SK, which can be the same as key K, (the required “unique key”). EX1004, 6:62-7:16, 9:32-36; EX1003, ¶¶232-234. In such an arrangement, the authorization and billing unit 13 can participate with the update unit 36 as the required “agent” that sets up the required “verification structure.” EX1003, ¶¶232-234.

- 30. Claim 16: “The method according to claim 13, wherein the step of verifying the program includes a decrypting the license record data accommodated in the erasable second non-volatile memory area of the BIOS using at least the unique key.”**

Hellman disclosed part of this element because it disclosed verifying the plaintext value M stored in the non-volatile memory 37 (the required “erasable second non-volatile memory area”) when the user attempts to use the software

package 17. EX1004, 10:33-65; EX1003, ¶¶235-237. A POSA would have found it obvious to store the authorization A instead of the plaintext value M as the required “license record” in the non-volatile memory 37. *See supra* § VII.B.5. A POSA would have recognized that with this modification, when the user attempts to use the software package 17, the encrypted license record (authorization A) in the non-volatile memory area of the BIOS (non-volatile memory 37, modified by Chou to store BIOS) would be decrypted in order to retrieve the value M. EX1003, ¶¶235-237. And because the authorization A was encrypted using the key K, a POSA would have understood that the key K would be used to decrypt the authorization A. EX1004, 6:62-7:2, 9:32-36; EX1003, ¶¶235-237.

VIII. THE BOARD SHOULD NOT EXERCISE ITS DISCRETION UNDER §§ 325(d) and 314(a) TO DENY REVIEW.

A. The substance of this Petition does not warrant denial under § 325 (d).

The Board has discretion to deny institution of *inter partes* review if “the same or substantially the same prior art or arguments previously were presented to the Office.” 35 U.S.C. § 325(d). *Becton, Dickinson* factors (a), (b), and (d) assess whether the same or substantially the same art or arguments previously were presented to the Office. *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019- 01469, Paper 6, 10 (P.T.A.B. Feb. 13, 2020) (precedential). They examine the similarities, material differences, and

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

cumulative nature of the asserted art and the prior art involved during examination (a, b,) as well as the extent of the overlap between arguments made during examination and those advanced by Petitioner or Patent Owner during this proceeding (d). *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8, 17–18 (P.T.A.B. Dec. 15, 2017) (precedential as to § III.C.5, first paragraph).

As the Board has already determined, none of these factors apply because Hellman, Chou, and Schneck were submitted to the Office for the first time in the since terminated TCT Mobile IPR, and are not cumulative. *See Sony Institution Decision* at 25–26.

B. The substance of this Petition also does not warrant denial under § 314(a)

The Board considers the factors set forth in both *General Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 at 16 (P.T.A.B. Sept. 6, 2017) (precedential as to § II.B.4.i) (“*General Plastic*”) and *Apple v. Fintiv*, IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020) (precedential) (“*Fintiv*”) to determine whether to exercise its discretion under § 314(a).

1. The *General Plastic* factors favor institution.

This Petition is not a coordinated serial attack that presents the kind of “undue inequities and prejudices” addressed by the Board’s precedent in *General Plastic*. *See General Plastic*, Paper 19 at 17–18. Since 2008, Patent

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

Owner Ancora has serially filed numerous patent infringement cases that assert the '941 Patent. *See* Sec. II. Mandatory Notices *supra*. A discretionary denial here under § 314(a) would unjustly disadvantage later IPR petitioners by precluding challenges to the '941 Patent that the Board has already determined to have at least a reasonable likelihood of success on the merits, but has never finally resolved. The substance and timing of this Petition do not present undue inequities, and the *General Plastic* factors do not favor denial.

Factor 1: Factor 1 considers whether the same petitioner previously filed a petition directed to the same claims of the same patent.” *Id.* at 16. This factor also applies to whether different petitioners have a “significant relationship.” *Valve Corp. v. Elec. Scripting Prods., Inc.*, IPR2019-00062, Paper 11 at 9-10 (P.T.A.B. Apr. 2, 2019) (precedential) (finding a “significant relationship” when a petitioner and prior petitioner “were co-defendants in the District Court litigation and were accused of infringing the [challenged] patent based on the [same] devices”).

Here, Petitioners have not previously filed any petition against the '941 Patent. Nor do Petitioners have any prior “significant relationship” with any of the prior petitioners with respect to the '941 patent that would implicate *General Plastic* or *Fintiv*.⁴

⁴ The TCT Mobile petition was filed by TCT Mobile (US) Inc., Huizhou TCL

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

This factor weighs in favor of institution and against discretionary denial.

Factors 2, 3, 4, and 5: These factors compare first- and second-filed petitions by the same petitioner. As explained above, Petitioners do not have a significant relationship with any other petitioners that filed prior IPR or CBM petitions challenging the '941 Patent. This is therefore Petitioners' first petition against the '941 Patent. Indeed, Petitioners only became aware of the '941 Patent, its litigation history, and the prior art presented in this Petition, *after* being served with a complaint for infringement by Patent Owner on July 20,

Mobile Communication Co., Ltd., and Shenzhen TCL Creative Cloud Technology Co., Ltd., mobile phone manufacturers, which were identified as the real parties in interest. Petitioner has never had any relationship with any of those parties. Petitioner Roku does have a relationship with a separate company, TCL Electronics Holdings Limited ("TCL Electronics"), but that relationship is irrelevant to any prior IPR Petition. TCL Electronics is one of many companies that makes smart televisions including proprietary Roku technology. Petitioner Roku was not a party to the parallel district court proceeding that precipitated the TCT Mobile petition, Roku's technology was not accused of infringement in the district court proceeding, Roku had not been put on notice of the '941 patent by Ancora, Roku had no notice of the TCT Mobile Petition, and Roku did not play *any* role in that district court proceeding or in the TCT Mobile IPR.

2021. (Factor 2). Petitioners are filing this Petition only 5 weeks after being served in the underlying parallel district court litigation. (Factor 4).

Factors 6 and 7: These factors examine the impact this petition would have on the Board's finite resources. This petition should have little impact on the Board's finite resources or its ability to issue a final determination on this Petition within one year because it is substantively identical—same grounds and same expert—as TCT's originally filed and instituted petition (IPR2020-01609) and Nintendo's recently filed and pending petition (IPR2021-01338). This streamlines the issues for the Board to reach a final determination within the statutory time limits. (Factors 6-7). Finally, Petitioner would be willing to confer with the Board to streamline issues with the Nintendo IPR, to the extent that would be useful.

2. The *Fintiv* factors favor institution.

The factors set forth in *Fintiv* also favor granting institution. *Fintiv* sets forth six factors for consideration:

Factor 1 (stays): Given the early stage of the proceedings, the district court has given no indication whether it would grant a stay, so this factor is neutral.

Factor 2 (timing re trial date): No trial date has been set and therefore no proximity to the projected statutory deadline for the PTAB's final written decision can yet be assessed, so this factor is neutral.

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

Factor 3 (investment in parallel proceeding): This Petition comes a mere five weeks after Patent Owner served Roku with a complaint alleging infringement of the '941 patent. As such, this Petition is timely and there has been limited, if any, investment in the district court litigation by the court and the parties. This factor therefore favors institution.

Factor 4 (overlap in substantive issues): There currently is no overlap in the issues between the proceedings at this time. Indeed, the Court recently extended Petitioners' deadline for responding to the complaint to September 8th and 9th, 2021, respectively. *Ancora Technologies, Inc. v. VIZIO, Inc.*, No. 6:21-cv-00739, Text Order Granting Motion for Extension of Time to Answer; *Ancora Technologies, Inc. v. Roku, Inc.*, No. 6:21-cv-00737 (same).

Factor 5 (identity of parties): Petitioners are the same as the defendants in the parallel district court litigation. (Factor 5). This factor therefore favors institution.

Factor 6: The Board has twice granted institution based on these same grounds over Ancora's contrary preliminary arguments. This indicates that the grounds are strong on the merits. *See Fintiv*, Paper 11 at 14-15 (noting that "particular strong" merits of a ground may serve the interest of overall system efficiency and integrity).

IX. CONCLUSION

As shown above, claims 1-3, 6-14, and 16 of the '941 Patent recite subject matter that was unpatentable over the prior art. Petitioners request institution of an *inter partes* review and cancellation of the claims.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

/Jon E. Wright/

Jon E. Wright
Registration No. 50,720
Attorney for Petitioners

Date: August 24, 2021

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

**CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION,
TYPEFACE REQUIREMENTS, AND TYPE STYLE REQUIREMENTS**

1. This Petition complies with the type-volume limitation of 14,000 words, comprising 13,965 words, excluding the parts exempted by 37 C.F.R. § 42.24(a).

2. This Petition complies with the general format requirements of 37 C.F.R. § 42.6(a) and has been prepared using Microsoft® Word 2016 in 14-point Times New Roman.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

/Jon E. Wright/

Jon E. Wright
Registration No. 50,720
Attorney for Petitioners

Date: August 24, 2021

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

Petition for Inter Partes Review of U.S. Patent No. 6,411,941

CERTIFICATION OF SERVICE (37 C.F.R. §§ 42.6(e), 42.105(a))

The undersigned hereby certifies that on August 24, 2021, true and correct copies of the foregoing **PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 6,411,941** and all associated exhibits were served in their entirety on the following parties via U.S.P.S. Priority Mail Express® or FedEx Express®:

Venable LLP
P.O. Box 34385
Washington, D.C. 20043-9998
PAIR Correspondence Address of Record for U.S. Patent No. 6,411,941

The above-captioned documents were also served electronically via e-mail on August 24, 2021 on the following parties:

Andres Healy
Lexie G. White
SUSMAN GODFREY LLP
ahealy@susmangodfrey.com
lwhite@susmangodfrey.com

Charles Ainsworth
Robert Christopher Bunt
PARKER, BUNT & AINSWORTH, P.C.
charley@pbatyler.com
rcbunt@pbatyler.com

Respectfully submitted,
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

/Jon E. Wright/

Jon E. Wright
Registration No. 50,720
Attorney for Petitioners

Date: August 24, 2021

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600