EXHIBIT B

A. Defendants' Proposed Constructions and Supporting Evidence for the Disputed Terms

Pursuant to P.R. 4-3(b), Defendants' proposed constructions and supporting evidence for the disputed terms of the '216 Patent are found in the following tables. Because Defendants' have not reached unanimous agreement on certain claim terms, competing constructions are provided in the various tables below. In addition, Pervasive Software, Inc. believes that the term "Licensee Unique ID" should be further modified by this Court and is moving for leave to provide a modification to the construction provided by the District of Rhode Island during the upcoming claim construction process:

Defendant Group A comprises all Defendants EXCEPT those found in Group B

	DISPUTED TERMS AND PHRASES	DEFENDANT GROUP A'S PROPOSED CONSTRUCTION	SUPPORTING EVIDENCE
1	Permits use of said digital data...only if...has matched . . .	When . . . has matched then the use of said digital data is permitted	"The algorithm in the code portion is duplicated at a remote location on a platform under the control of the licensor or its agents, and communication between the intending licensee and the licensor or its agent is required so that a matching registration number can be generated at the remote location for subsequent communication to the intending licensee as a permit to licensed operation of the digital data in a use mode." '216 patent, Abstract. "In broad terms, the system according to the invention is designed and adapted to allow digital data or software to run in a use mode on a platform if and only if an appropriate licensing procedure has

	DISPUTED TERMS AND PHRASES	DEFENDANT GROUP A'S PROPOSED CONSTRUCTION	SUPPORTING EVIDENCE
			been followed." '216 patent, col. 2:52-55. "Accordingly, in one broad form of the invention there is provided a system for licensing use of digital data in a use mode, the digital data executable on a platform, the system including local licensee unique ID generating means and remote licensee unique ID generating means, the system further including mode switching means operable on the platform which permits use of the digital data in the use mode on the platform only if a licensee unique ID generated by the local licensee unique ID generating means has matched a licensee unique ID generated by the remote licensee unique ID generating means." '216 patent, col. 3:22-32. "In a further broad form of the invention, there is provided a method of control of distribution of software, the method comprising providing mode-switching means associated with the software adapted to switch the software between a fully enabled mode and a partly enabled or demonstration mode; the method further comprising providing registration key generating means adapted to generate an enabling key which is a function of information unique to an intending user of the software; the mode-switching means switching the software into fully enabled mode only if an enabling key provided to the mode-switching means by the intending user at the time of registration of the software has matched identically with the registration key generated by the

	DISPUTED TERMS AND PHRASES	DEFENDANT GROUP A'S PROPOSED CONSTRUCTION	SUPPORTING EVIDENCE
			registration key generating means." '216 patent, col. 4:30-43. "Preferably, the registration code when executed on the platform provides local licensee unique ID generating means whereby the digital data can be switched from the demonstration mode to the use mode by execution of the registration code only if a licensee unique ID generated by the local licensee unique ID generating means has matched a licensee unique ID generated by remote licensee unique ID generating means." '216 patent, col. 4:55-62. "FIGS. 2a, 2b and 2c are segments of a flow chart of the procedure to be followed during registration of software by a user according to a first embodiment of the invention." '216 patent, col. 5:5-7; *see also* Figs. 2a, 2b and 2c and accompanying text at col. 6:34 – 8:38. "FIG. 8 is a block diagram of a generalized system according to a fifth embodiment of the invention." '216 patent, col. 5:20-21; *see also* Fig. 8 and accompanying text at col. 11:39 – 12:37. "It is to be understood that, in its various embodiments, the present invention is for the protection of digital code/software by control of permission to use the digital code/software." '216 patent, col. 5:33-36.

	DISPUTED TERMS AND PHRASES	DEFENDANT GROUP A'S PROPOSED CONSTRUCTION	SUPPORTING EVIDENCE
			"With reference to FIGS. 1 and 8, the system according to embodiments of the invention is designed and adapted to allow digital data 39 or software to run in a use mode on a platform 31 if and only if an appropriate licensing procedure has been followed." '216 patent, col. 5:47-51. "As a final stage in registration (refer to FIG. 2d [sic – 2c]), the registration authority 16 provides the registration number generated by the registration authority PC 15 to the user 11. The user 11 enters the registration number into the user PC 12 where the registration routine checks to see whether the entered registration number matches the calculated registration number. If the two match, then a valid registration has taken place and access is provided by the registration routine to a full operating version of the software protected by the registration routine. If there is no match and a preference file (which stores the user details) does not exist then a dialogue box D (FIG. 2c) appears on the display 13 of user PC 12 providing the prospective new user 11 with the opportunity to check his/her details or switch to the demonstration version of the software protected by the registration routine." '216 patent, col. 7:36-50. "When mode switcher 68 verifies the match, then the mode switcher 68 allows execution on platform 31 of the full user program 39." '216 patent, col. 11:63-65. "Second gate 92 permits execution of any kind of

	DISPUTED TERMS AND PHRASES	DEFENDANT GROUP A'S PROPOSED CONSTRUCTION	SUPPORTING EVIDENCE
			code by closure of relay 93 provided only that the output of comparator 90 is high (which is to say that X equals Y or that the local licensee unique ID matches with the licensee unique ID generated by the remote licensee unique ID generating means comprising summer 89)." '216 patent, col. 13:31-36. "Because additional information is added at the remote computer in Grundy, it follows automatically that a simple comparison or match of the registration code derived from the local computer and the authorization code derived from the remote computer is not possible. In order for the local computer to deem the authorization code as valid, the local computer is required to somehow take account of the additional information which has been added by the remote computer. Grundy does not describe precisely how this is achieved, but it is clear that the validity of the authorization code of Grundy cannot be determined as a simple <u>match</u> of the registration code with the authorization code. Accordingly, Claim 1 of the present application which requires a <u>match</u> of the local license unique ID with the remote licensee unique ID is patentably distinguished over the fundamentally more complex process outlined in Grundy." '216 file history, 12/21/94 Amendment in Response to June 24, 1994 Office Action at 4-5. "It is not at all clear from the disclosure of Grundy as to whether the previously derived "Registration Code" is ever utilized to help check the validity of the

	DISPUTED TERMS AND PHRASES	DEFENDANT GROUP A'S PROPOSED CONSTRUCTION	SUPPORTING EVIDENCE
			Authorization Code: one is perfectly entitled to infer from the total disclosure of Grundy that any element of uniqueness to be associated with the software to be protected is injected and derived at the second platform (the remote location) and, furthermore, that whether an Authorization Code is valid or not derives directly from data first arising at the second platform (the remote location). This is the complete reverse of the system of the present invention where the uniqueness derives entirely locally." '216 file history, 7/5/95 Amendment in Response to March 30, 1995 Office Action at 7. "In addition, the Grundy system requires a mechanism for encrypting the registration code for its return trip from the second platform to the first platform: Applicant respectfully submits that the encryption key is the 'User Code' generated at the second platform. Without the communication of the encryption key (the user code) to the first platform it will not be possible to decrypt the authorization code and hence, it will not be possible to make any use of the authorization code for validation purposes. Advantageously, the system of the claimed invention does not require that an encryption key be passed from the second platform to the first platform. The Examiner states that 'the Grundy local decodes the authorization code which then must match the original user data.' It is respectfully submitted that Grundy does not disclose a mechanism for decoding the authorization code, hence it follows that Grundy

	DISPUTED TERMS AND PHRASES	DEFENDANT GROUP A'S PROPOSED CONSTRUCTION	SUPPORTING EVIDENCE
			does not disclose a mechanism by which there can be a match with original user data. Therefore, by a mechanism not specifically disclosed in Grundy, the 'Unique User Code' must, somehow, be communicated to the first platform because it amounts to a decryption key without which no useful information can be derived from the authorization code. By contrast, the invention of the present application does not require any decryption key to pass from the second platform (the remote location) to the first platform (the local location) because the same algorithm is used at both locations. This feature is now clearly included in all proposed main claims, and, it is submitted, patentably distinguishes the present invention over Grundy." '216 file history, 7/5/95 Amendment in Response to March 30, 1995 Office Action at 8-9; *see also id.* at 6-7. "The local and remote licensee unique IDs are compared and if they match identically, the system will allow licensed operation (e.g., full, unrestricted use) of the software." '216 reexam history, 11/29/10 Reply to Office Action in Ex Parte Reexamination at 12. "If the remote licensee unique ID identically matches the local licensee unique ID then the system will allow licensed operation of the software." '216 reexam history, 11/29/10 Declaration of Ric B. Richardson Under 37 C.F.R. § 1.132 at ¶ 6.

	DISPUTED TERMS AND PHRASES	DEFENDANT GROUP A'S PROPOSED CONSTRUCTION	SUPPORTING EVIDENCE
			"Of the other art of record, the only one that suggests that use of user-specific information in the computation of fields is Grundy. The Patent Owner has persuasively argued that the summation disclosed by Grundy is used in the context of merely verifying the correctness of information related to the user and is not being used to generate an ID per se. Since the information is not being used for the same purpose, one skilled in the art therefore would not use the algorithm of Grundy as part of the generation of the claimed licensee unique ID." '216 reexam history, 8/5/2011 Notice of Intent to Issue Ex Parte Reexamination Certificate at 6.
2	Local (in the phrase "local licensee unique ID generating means")	On the user's computer executing the digital data	Local licensee unique ID shown at "Local Licensee Location." '216 patent, FIG. 8. "an environment to be associated with a computing device such as a microprocessor or other data processing device which permits execution of the digital data…." '216 patent, col. 2:25-27. "The prospective new user 11 inserts disk 10 into the user PC 12 so as to be read by PC 12." '216 patent, col. 6:39-41. "This information, unique to the user, is passed through a registration number algorithm 14… which generates a registration number…." '216 patent, col. 7:14-17.

	DISPUTED TERMS AND PHRASES	DEFENDANT GROUP A'S PROPOSED CONSTRUCTION	SUPPORTING EVIDENCE
			"The distinction as against the first embodiment is that the 'key file' is created at the time of registration of the software and a duplicate key file is also created at the same time." '216 patent, col. 8:50-53. "… form a microprocessor 30 adapted to operate under an operating system or upon a platform 31 such as, for example MicroSoft DOS or Macintosh System 7." '216 patent, col. 10:18-20. "The digital data 37 is arranged in such a way that when microprocessor 30 seeks to first execute the digital data 37 by way of operating system or platform 31 the digital data comprising the registration code portion 38 is caused to execute first…." '216 patent, col. 10:30-34. "[T]he algorithm, which generates the unique user identification and which is resident both as a the registration code portion 38 in digital data 37 integrally bound to use code portion 39 for execution on local platform 31 and also as remote algorithm 61…." '216 patent, col. 11:46-50. "[A] prospective user 80 of digital code 81 on media 82 by its execution on platform 83 firstly inserts the media 82 into an appropriate digital code reading device within the platform…." '216 patent, col. 12:46-49. "[T]he Applicant submits herewith redrafted claims,

	DISPUTED TERMS AND PHRASES	DEFENDANT GROUP A'S PROPOSED CONSTRUCTION	SUPPORTING EVIDENCE
			the main claims of which include, broadly, the following two distinguishing limitations: (a) The 'Licensee Unique ID' on which the registration system relies for matching for verification purposes is generated locally…." '216 file history, 6/30/95 Response at 6. "[T]he 'Licensee Unique ID' is entirely the product of data generated locally as distinct from data added before delivery of the software to the local location for use… or subsequently from a remote location…." '216 file history, 6/30/95 Response at 6-7. "A direct comparison for matching purposes of the licensee unique ID at the local location…." '216 file history, 6/30/95 Response at 8. Pic of "local system" which is a user's computer containing local licensee unique ID. '216 reexam history, Slide 5 of Presentation at1087. "Local Licensee Unique ID Generation" is "A unique identification generated locally…." '216 reexam history, Slide 7 of Presentation at1089. "[P]roduced locally and remotely." '216 reexam history, Slide 31 of Presentation at1113.

	DISPUTED TERMS AND PHRASES	DEFENDANT GROUP A'S PROPOSED CONSTRUCTION	SUPPORTING EVIDENCE
3	Comprises part of said digital data when executed on said platform	Entirely contained in said digital data when executed on said platform	"A registration system allows digital data or software to run in a use mode on a platform if and only if an appropriate licensing procedure has been followed. Preferably, the system detects when part of the platform on which the digital data has been loaded has changed in part or in entirety, as compared with the platform parameters, when the software or digital data to be protected was last booted or run. The system relies on a portion of digital data or code which is integral to the digital data to be protected by the system. This integral portion is termed the code portion and may include an algorithm that generates a registration number unique to an intending licensee of the digital data based on information supplied by the licensee which characterizes the licensee." '216 patent, Abstract. "The system relies on digital data or code which forms part of the digital data to be protected by the system. This portion of the digital data which preferably is integral to the digital data to be protected has been termed the 'code portion' elsewhere in this specification. The code portion includes an algorithm adapted to generate a registration number which is unique to an intending licensee of the digital data based on information supplied by the licensee which characterizes the licensee." '216 patent, col. 2:61-3:2.

	DISPUTED TERMS AND PHRASES	DEFENDANT GROUP A'S PROPOSED CONSTRUCTION	SUPPORTING EVIDENCE
			"Preferably, the code portion is integral with the digital data and can be identical for all copies of the digital data. It is the algorithm embedded within the code portion (and which is duplicated at the remote location) which provides a registration number which can be 'unique' if the information provided by the intending licensee upon which the algorithm relies when executed upon the platform is itself 'unique.'" '216 patent, col. 3:10-17. "Accordingly, in one broad form of the invention there is provided a system for licensing use of digital data in a use mode, the digital data executable on a platform, the system including local licensee unique ID generating means and remote licensee unique ID generating means, the system further including mode switching means operable on the platform which permits use of the digital data in the use mode on the platform only if a licensee unique ID generated by the local licensee unique ID generating means has matched a licensee unique ID generated by the remote licensee unique ID generating means." '216 patent, col. 3:22-32. "Preferably, the platform unique ID generating means forms part of the digital data." '216 patent, col. 3:54-55.

	DISPUTED TERMS AND PHRASES	DEFENDANT GROUP A'S PROPOSED CONSTRUCTION	SUPPORTING EVIDENCE
			"The system relies on digital data or code 38 which forms part of the digital data to be protected by the system. This portion of the digital data, which preferably is integral to the digital data to be protected, has been termed the code portion 38 elsewhere in this specification. The code portion 38 includes an algorithm adapted to generate a registration number 66 or local licensee unique ID or registration key which characterizes the licensee. In this instance, the local licensee unique ID generator which generates the registration number comprises the execution of code 38 on platform 31." '216 patent, col. 3:57-67. "Preferably, the code portion 38 is integral with the digital data and can be identical for all copies of the digital data. It is the algorithm embedded within the code portion (and which is duplicated at the remote location) which provides a registration number which can be 'unique' if the information provided by the intending licensee upon which the algorithm relies when executed upon the platform is itself 'unique'." '216 patent, col. 6:15-22. "The digital data 37 includes registration code portion 38 and use code portion 39." '216 patent, col. 10:28-29, and Figure 5.

	DISPUTED TERMS AND PHRASES	DEFENDANT GROUP A'S PROPOSED CONSTRUCTION	SUPPORTING EVIDENCE
			"It will be appreciated that the registration code portion 38 effectively forms simply a part of the software or digital data 37 to be protected/registered and that the digital data 37 will be or can be identical for all copies of the word processing program produced. The registration code portion 38 allows a unique link to be made between the digital data 37 and an individual authorized or licensed to use the digital data 37 by way of initial execution of a copy of the digital data comprising registration code portion 38." '216 patent, col. 10:53-61, and Figure 5. "The system illustrated in FIG. 8 operates in the manner generally described in respect of previous embodiments and as generally outlined in the diagram. In the context of the block C illustrated in FIG. 4, and with reference to FIG. 9, the algorithm, which generates the unique user identification and which is resident both as the registration code portion 38 in digital data 37 integrally bound to use code portion 39 for execution on local platform 31 and also as remote algorithm 61, is attached to registration database program 62 for execution on the remote platform 63." '216 patent, col. 11:43-52, and Figure 8.

	DISPUTED TERMS AND PHRASES	DEFENDANT GROUP A'S PROPOSED CONSTRUCTION	SUPPORTING EVIDENCE
4	Prosecution History Disclaimer Applicable To All Claims	The licensee unique ID/security key cannot be generated by a checksum, summation algorithm, summer, or equivalent thereof, used to test data integrity.[1]	See Attachment 1 To Exhibit B

Defendant Group B (comprising Defendants Aspyr Media, Inc., Borland Software Corp., Digital River, Inc., GEAR Software, Inc. and GEAR Software Holdings, Inc.)

	DISPUTED TERMS AND PHRASES	DEFENDANT GROUP B'S PROPOSED CONSTRUCTION	SUPPORTING EVIDENCE
Note: Defendant Group B incorporates herein the proposed constructions and supporting evidence for disputed terms and phrases 1 through 4 noted above, and adds the following prosecution history disclaimer.			
5	Prosecution History Disclaimer Applicable To All Claims	The licensee unique ID generated by the means recited in each of the claims must be derived from at least one piece of information that is specific to the user, such as name, billing information, or product information unique to the installation entered by the user. The information cannot be specific to the computer or independently generated by the computer.[2]	See Attachment 2 to Exhibit B

[1] By arguing that there has been a disclaimer based on the reexamination file history, the Defendants maintain, and do not waive, the additional argument that, independent of the disclaimer, the claims as previously construed do not cover the disclaimed subject matter.

[2] By arguing that there has been a disclaimer based on the reexamination file history, the Defendants maintain, and do not waive, the additional argument that, independent of the disclaimer, the claims as previously construed do not cover the disclaimed subject matter.

ATTACHMENT 1 TO EXHIBIT B

(Evidentiary Support For Prosecution History Disclaimer)

Intrinsic Evidence in support of the following disclaimer from the reexamination file history: ***the licensee unique ID/security key cannot be generated by a checksum, summation algorithm, summer, or equivalent thereof, used to test data integrity***.

- Grundy does not cure this deficiency of Hellman. The Office alleges that the unique identifier associated with the licensee is disclosed by Grundy's "checksum." ***But Grundy's checksum is solely used to verify the accuracy of user-entered information-it is not a unique identifier associated with a licensee***.

  (Reply to Office Action, filed Nov. 29, 2010, p. 18 (emphasis added)).

- ***Thus, Grundy's "checksum" is not uniquely associated with an intended licensee***. Rather, Grundy's checksum can only be used to indicate whether the user (i.e., the intended licensee) correctly entered the requested data.

  (Reply to Office Action, filed Nov. 29, 2010, pp. 18-19 (emphasis added)).

- However, Grundy's checksum cannot meet these limitations as it cannot be equated to claim 1's "licensee unique ID." As explained more fully below, ***Grundy's checksum is used for nothing more than verifying that the licensee correctly entered data. It is not uniquely associated with any intended licensee and cannot be used to identify any intended licensee***.

  (Reply to Office Action, filed Nov. 29, 2010, p. 26 (emphasis added)).

- Thus, Grundy uses the checksum of the user data as an indicator that the user data has been correctly entered. ***Grundy does not teach or suggest that the checksum***, or the registration code that includes the checksum as one of the fields, ***represents a unique identifier associated with intended registered user***.

  (Reply to Office Action, filed Nov. 29, 2010, p. 27 (emphasis added)).

- ***A person of ordinary skill in the art would understand "checksum" to represent a small number of check digits that are typically appended to data in order to ensure the data's integrity when it is stored or transmitted***. To calculate a checksum of some data, the data is added up (e.g., broken up into C-byte chunks, where C is a small number such as 1, 2, 4, or 8, and summed); the sum is chopped to a fixed length (e.g., a byte or C bytes) and appended to the data before storage or transmission. Checksum algorithms used in practice are variations on this scheme. When the data is received or retrieved later, the checksum is re-calculated to ensure that the result is the same as the original checksum; if the result differs then the data must have been corrupted. (See, Rosenblatt Dec., ¶52.)

  (Reply to Office Action, filed Nov. 29, 2010, p. 27 (emphasis added)).

- ***A checksum is therefore much smaller in length than its input data.*** For example, a 16-bit (2-byte) or 64-bit (8-byte) checksum may be calculated on thousands, millions, or billions of bytes of data. ***This fulfills the checksum's intended purpose well, given that most errors in data storage or transmission are small and localized, making it highly likely that the resulting checksum will differ from the one originally calculated, and extremely unlikely that corrupted data will produce the same checksum as the original one.*** For example, if one or two bits are altered, the checksum will differ. (See, Rosenblatt Dec., ¶56.)

  (Reply to Office Action, filed Nov. 29, 2010, p. 27 (emphasis added)).

- Therefore, ***a checksum cannot preserve the uniqueness of the input data***. Grundy shows the input data to the checksum routine in Fig. 2, 212, "ENTER NEW USER DETAILS." This is "new user data, such as the user's name, address and telephone number" (Grundy at 12:37-38.) Such data might take up roughly a hundred bytes of data. ***A checksum of this data would not preserve its uniqueness; many different sets of user data could produce the same checksum. Therefore the checksum is not a generator of unique identifiers***. (See, Rosenblatt Dec., ¶62.)

  (Reply to Office Action, filed Nov. 29, 2010, p. 27 (emphasis added)).

- As previously discussed, ***a checksum cannot preserve the uniqueness of the input data and thus the checksum is not a generator of unique identifiers***. (See, Rosenblatt. Dec., 62.)

(Reply to Office Action, filed Nov. 29, 2010, p. 32 (emphasis added)).

- But as fully discussed above with respect to independent claim 1, ***a checksum is not unique and therefore cannot be a unique identifier associated with a licensee***. Specifically, ***Grundy is not using the checksum to represent a security key, but rather uses the checksum of the user data as an indicator that the user data has been correctly entered***. ***Grundy does not teach or suggest that the checksum represents a unique identifier of an intended registered user***.

  (Reply to Office Action, filed Nov. 29, 2010, p. 33 (emphasis added)).

- "These fields, however, are checksums. Checksums are not unique fields, even if there [sic] are at least in part derived from unique data. It is NOT agreed that a reasonable examiner would have found this reference important in determining the patentability of claims 1-20." (Order Granting/Denying Request for Ex Parte Reexamination, pg. 9, emphasis added)

  Patent Owner Agrees

  (Uniloc Powerpoint slides presented to Examiner during Nov. 17, 2010 Examiner Interview, slide 36).

- ***Checksum is not unique and does not uniquely identify an intended registered user***

  (Uniloc Powerpoint slides presented to Examiner during Nov. 17, 2010 Examiner Interview, slide 37).

- Uniloc submits that based on the Examiner's statement in the Order, ***Grundy's data validation checksums do not produce a unique ID*** that could be used by Hellman.

  (Reply to Office Action, filed Mar. 18, 2011, p. 15).

- Uniloc also argued that Grundy's checksum did not generate "a licensee unique ID" because Grundy's checksum algorithm, by its very nature, destroys any uniqueness.

  (Reply to Office Action, filed Mar. 18, 2011, p. 16).

- As Dr. Pooch explains that "Grundy ... describes several conventional uses for checksums." (Pooch Dec. 8.) For example, "***the checksums described in Grundy are not cryptographic functions, but rather appear to be used to check, for example, for typographical data entry errors or transmission errors***." (Pooch Dec., 32.)

  (Reply to Office Action, filed Mar. 18, 2011, p. 31).

- In the rejection of claim 1 on page 14, on the other hand, the Examiner proposes to replace Hellman's cryptographic function generator 38 with the checksum of Grundy to provide the summation algorithm limitation absent from the teachings of Hellman. (Second Action, p. 15; bottom.) ***However, if these references are combined as the Examiner suggests, with Grundy's error-checking checksum replacing Hellman's cryptographic function generator, the Examiner can no longer take credit for the "uniqueness" feature provided by Hellman because the source of that uniqueness, the one-way compressive hash function having a 100:1 X/Y bit ratio, would also be replaced by Grundy's checksum***. Uniloc therefore requests that the obviousness rejection of claims 2, 12 and 1 7 be reconsidered and withdrawn.

  (Reply to Office Action, filed Mar. 18, 2011, p. 34).

- The basis for this determination was that the Requester attempted to rely on Grundy's checksums; and, according to the Office, Grundy's "***[c]hecksums are not unique fields, even if there [sic] are at least in part derived from unique data.***" (Order, p. 9.)
  Yet despite this ***technically correct*** analysis of Grundy's checksums …

  (Reply to Office Action, filed Mar. 18, 2011, p. 43).

- Further, the checksums described in Grundy are not cryptographic functions, but rather appear to be ***used to check for typographical data entry errors or transmission errors***.

  (Declaration of Dr. Udo W. Pooch Under 37 C.F.R. § 1.132, ¶ 32).

- ***While the usual checksums are useful in detecting accidental modification such as corruption to stored data or errors in a communication channel, they provide no security against a malicious agent as their simple mathematical structure makes them trivial to circumvent. To provide this level of integrity, the use of a cryptographic hash function is necessary***.

  (Declaration of Dr. Udo W. Pooch Under 37 C.F.R. § 1.132, ¶ 33).

- A checksum is a value that (a) is computed by a function that is dependent on the contents of a data object and (b) is stored or transmitted together with the object, for the purpose of detecting changes in the data. A checksum algorithm is a signature algorithm that does not

attempt to provide cryptographic protection against inversion. The term "checksum" originally referred to checking algorithms that summed the bytes, but is now generally used to refer to any non-cryptographic checking algorithm.

(Declaration of Dr. Udo W. Pooch Under 37 C.F.R. § 1.132, ¶ 36).

- This is consistent with a contemporaneous definition of "checksum" from the time the application leading to the '216 patent was filed, which defines a "checksum" as:

  a calculated value that is used to test data integrity. Errors can occur when data is transmitted or when it is written to disk. One means of detecting such errors is use of a checksum, a value calculated for a given chunk of data by sequentially combining all the bytes of data with a series of arithmetic or logical operations. After the data is transmitted or stored, a new checksum can be calculated (using the possibly faulty transmitted or stored data) and compared with the original one. If the checksums don't match, an error occurred, and the data should be transmitted or stored again; if they do match, the transmission or storage was probably error-free. Checksums are a simple validation mechanism, and they cannot be used to correct erroneous data.

  (Declaration of Dr. Udo W. Pooch Under 37 C.F.R. § 1.132, ¶ 36 (citing Computer Dictionary, The Comprehensive Standard for Business, School, Library, and Home, Microsoft Press (1991) (emphasis added)); see also Pooch Declaration at ¶¶ 37-38.

- Declaration of William R. Rosenblatt Under 37 C.F.R. § 1.132, filed Nov. 29, 2010, ¶¶ 48-65. (See, for example, ¶ 51: "I concur with that characterization of checksums. ***A checksum is not usable as a generator of unique IDs***." See also, for example, ¶ 63: "For the above reasons, ***a checksum cannot possibly preserve whatever uniqueness the input data may possess***. In particular, a POSA would not ascribe any reasonable definition of 'unique' to the output of a checksum routine.")

- The PTO relied on Uniloc's repeated and express disclaimers by stating (inter alia): The Patent Owner has persuasively argued that the summation disclosed in Grundy is used in the context of merely verifying the correctness of information related to the user and is not being used to generate an ID per se. Since the information is not being used for the same purpose, one skilled in the art therefore would not use the algorithm of Grundy as part of the generation of the claimed licensee unique ID." (Notice of Intent to Issue Ex Parte Reexamination Certificate, at p. 6.)

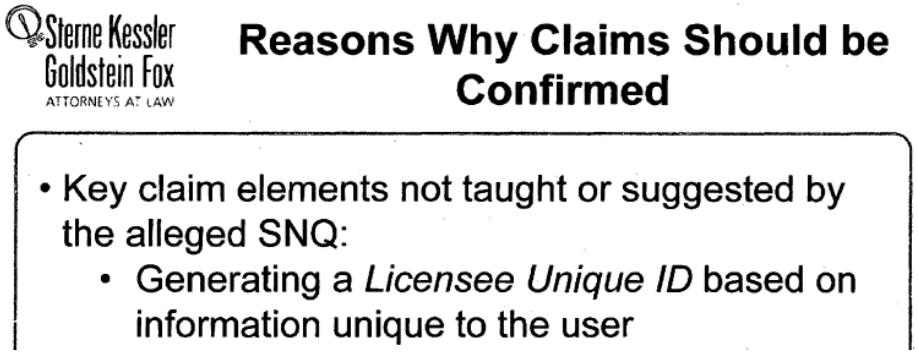
- Defendants may rely on other statements made by Uniloc during the reexamination, as well other specific statements made by the declarants in the declarations submitted by Uniloc during the reexamination. In addition, Defendants note that Uniloc has just produced, on August 29, 2011, the lengthy declaration of William Rosenblatt. While Defendants have cited to certain portions of that declaration, above, Defendants reserve the right to rely on other portions of that declaration, which appears to include extensive support for the disclaimer.

ATTACHMENT 2 TO EXHIBIT B

(Evidentiary Support For Prosecution History Disclaimer)

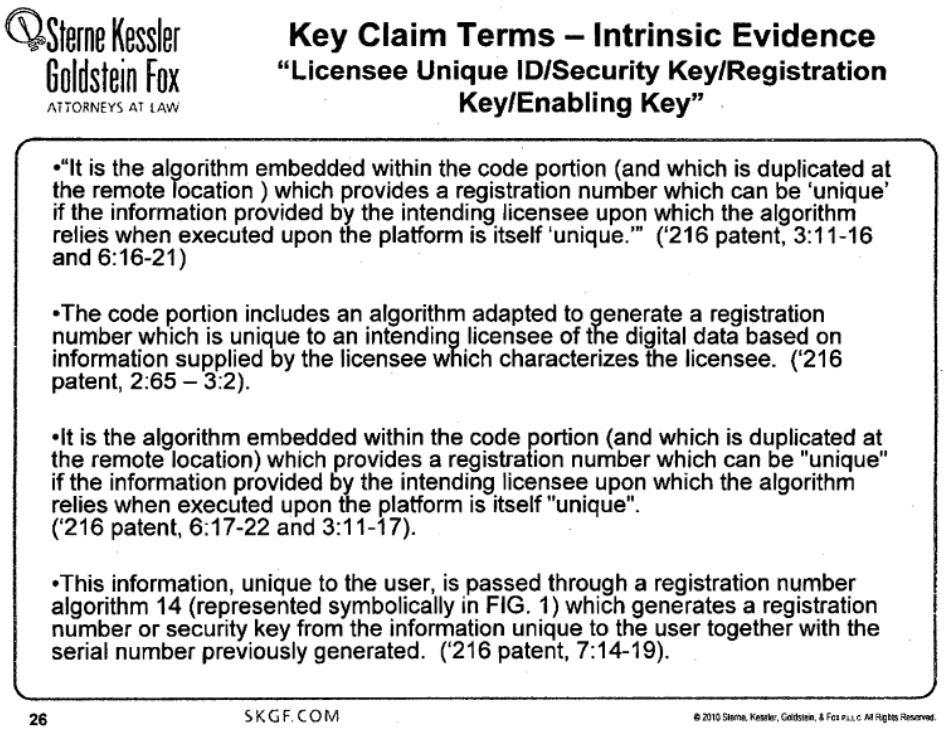
Intrinsic Evidence in support of the following disclaimer from the reexamination file history: ***The licensee unique ID generated by the means recited in each of the claims must be derived from at least one piece of information that is specific to the user, such as name, billing information, or product information unique to the installation entered by the user. The information cannot be specific to the computer or independently generated by the computer.***[3]

Ex Parte Reexamination Interview Summary, mailed on Nov. 19, 2010, slide 22:



Id. at slide 26:

[3] By arguing that there has been a disclaimer based on the reexamination file history, the Defendants maintain, and do not waive, the additional argument that, independent of the disclaimer, the claims as previously construed do not cover the disclaimed subject matter.



Id. at slides 32-35:

Sterne Kessler Goldstein Fox
ATTORNEYS AT LAW

Hellman Does Not Disclose a *Licensee* Unique ID (as testified at trial by Professor Hellman)

"The Hellman patent, however, does not use a product key or any other "non-platform-related" user information to create a licensee unique ID. ... Hellman (the person) *admitted* – after repeatedly being impeached with his deposition testimony – that his patent failed to teach this requirement of the claims."
(Yellow Brief – Uniloc USA v. Microsoft, Case No. 2010-1035-1055 (Fed. Cir.), p. 57)

[Attorney] Question: If you wanted to indicate that information associated with the user, unique information was input into the cryptographic function, you certainly had the ability to disclose that in the figures, if you so chose.
[Hellman] Answer: Correct.
[Attorney] Question: And you didn't?
[Hellman] Answer: Correct.
[Attorney] Question: And you also had the ability to describe in the patent, if you so chose?
[Hellman] Answer: In the specification? Yes.
[Attorney] Question: And you didn't?
[Hellman] Answer: Correct
(March 31, 2009 Trial Transcript: p.61, ll. 17 - p 62, ll. 4, Uniloc USA, Inc. et al. v. Microsoft Corp., C.A. No. 03-440 (D.R.I.))

Sterne Kessler Goldstein Fox
ATTORNEYS AT LAW

Hellman Does Not Disclose a *Licensee* Unique ID

- K is a base unit identifying key stored in permanent memory, inaccessible by the user
- N is the number of software uses being requested
- R is a random number
- H is a value that identifies the name of the software package being requested
- ***None of the above are associated with the licensee (as admitted by Hellman at trial)***

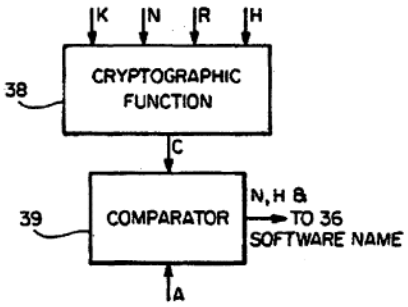


FIG_7

Sterne Kessler Goldstein Fox
ATTORNEYS AT LAW

Hellman Does Not Disclose Local *Licensee Unique ID*

K, N, R, and H are used to generate C. However C is not disclosed to be a unique ID associated with a user. Therefore C is not a "**licensee unique** ID" as recited in claims 1, 19 and 20. Nor is C "a security key [generated] from information input to said software which **uniquely identifies** an intended registered **user**" as recited in claim 12, nor is C "a registration key which is a function of information **unique** to an intending **user** of the software" as recited in claim 17.

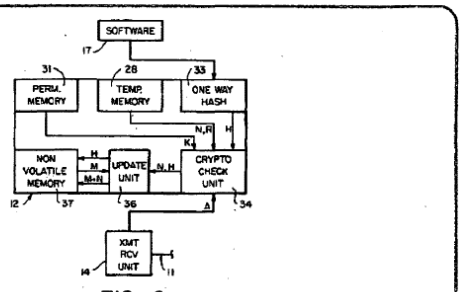


FIG_6

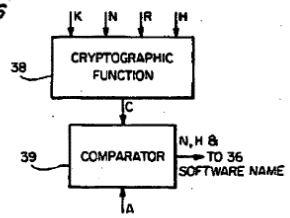


FIG_7

35 SKGF.COM

Office Action Response filed Nov. 29, 2010, at 17-18, 20-25, 29, 31, and 33-35.

See, e.g., id. at 17:

> Rather than describe any unique identifier that is associated with an intended licensee, Hellman instead describes a "method and apparatus in which use of the software can be authorized for a particular base unit a specific number of times." (*See,* Hellman 4:38-40.)

See e.g., id. at 18:

Therefore, Hellman discloses an authorization system for use of a software program based on a key identifier associated with a base unit, e.g., a personal computer. That identifier is generated by the manufacturer of the base unit and is not associated with the user, or intended licensee of the software program.

Hellman further teaches that "base unit 12 generates and communicates to authorization and billing unit 13 a signal representing a user originated request for software use," where "[t]his request consists of several parts SOFTWARE NAME, SERIAL NUMBER, N, R, and BILLING INFORMATION. (Hellman, 5:57-61.) Hellman defines these terms where "SOFTWARE NAME is the name of the software package to be used;" "SERIAL NUMBER is a serial number, identification, user name or similar identifier unique to base unit 12;" "N is the number of additional uses of software requested;" and "R is a random number, counter value, or other non-repeating number generated by the base unit 12." (Hellman 5:62-68.) As described more fully below, the "request" and "authorization" are based upon information regarding the desired software program to be authorized, the number of uses the software package is to be authorized, a non-unique random number, and a serial number unique to the computer base unit. Therefore, Hellman fails to teach or suggest a unique identifier that is associated with a licensee.

See, e.g., id. at 20:

(a) Hellman Does Not Teach or Suggest the "Licensee Unique ID" of Claim 1

As discussed above, the term "licensee unique ID" should be construed as "a unique identifier associated with a licensee." Hellman fails to disclose an identifier associated with a ***licensee***. Hellman also fails to disclose an identifier associated with a licensee that is also ***unique.***

See, e.g., id. at 21:

However, as discussed next, none of the input signals to Hellman's cryptographic function generator 38 (or 23)—namely, K (or SK), N, R and H—are unique to a licensee and therefore cannot disclose the "local licensee unique ID" of claim 1.

See, e.g., id. at 22-23:

Hellman's FIG. 7 "depicts an implementation of the cryptographic check unit 34," where "[s]ignals representing K, N, R, and H are applied as inputs to a cryptographic function generator 38 which generates a check value C as an output signal." (Hellman 10:14-18 and FIG. 7 below.)

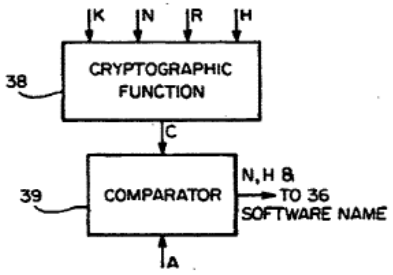


FIG_7

None of the inputs to the cryptographic function 38 is a unique identifier associated with a licensee, as required by the claimed "licensee unique ID." (See, Rosenblatt, ¶¶41-47.) For example, Hellman discloses that "the base unit 12 has a base unit key, K, stored in a permanent memory 31, for example a PROM which is burned in during manufacture of the base unit." (Hellman, 9:29-32.) Hellman further discloses that "where K and SK are equal to one another," that "[i]n that case K must be stored in a secure memory, inaccessible to the

user," as "if the user can learn K, in this case he has learned SK, and he can generate authorizations to himself to use any software package without paying for its use." (Hellman, 9:36-40.) Thus, K is a number associated with the base unit that is purposely withheld from the user. (See, Rosenblatt, ¶38.) K is therefore not uniquely associated with an intended licensee.

Nor are inputs H, R or H. Hellman discloses that the next input "N" is "the number of additional uses of software requested." Like K, N is not uniquely associated with an intended licensee. The next input "R" is "a random number." A random number is not uniquely associated with an intended licensee. The next input "H" is "used as an 'abbreviation' or name for describing the software package 21," where "any two software packages with the same H value are considered equivalent." (Hellman, 5:65 - 6:45.) Input "H," like N and R, is also not uniquely associated with an intended licensee.

In sum, the signals representing K, N, R, and H are applied as inputs to cryptographic function generator 38 which generates a check value C as an output signal. None of these signals are uniquely associated with the licensee and the resulting value C therefore cannot be equated to the claimed "licensee unique ID" of independent claim 1. (Rosenblatt Dec., ¶¶36-47.)

See, e.g., id. at 24:

Like the local version, Hellman uses four inputs to generate authorization signal "A" in the remote cryptographic function generator 23. These four inputs consist of H, R, N, and SK, are also not uniquely associated with the intended licensee. Inputs H, R, and N are the same as described above with respect to the local cryptographic function generator 38 and are not uniquely associated with the licensee. The remaining input signal, SK, is "obtained from authorization and billing unit's table of serial numbers and secret keys." (Hellman 7:1-2.) SK is a base unit's secret key where "[a]uthorization and billing unit 13 contains a memory 18 having a table of serial numbers and secret keys which allows authorization and billing unit 13 to determine a based unit's secret key, SK, from knowledge of the base unit's public serial number." (*See,* Hellman 6:19-21.) (*See,* Rosenblatt Dec., ¶38.) SK is therefore not uniquely associated with an intended licensee.

See, e.g., id. at 25:

As a final matter, Uniloc's position on Hellman was further substantiated by sworn testimony given by the inventor himself, Professor Martin E. Hellman on March 31, 2009 during the *Uniloc USA, Inc. et al. v. Microsoft Corp.* Rhode Island District Court trial. During trial Professor Hellman was questioned concerning his patent on whether he intended to associate user information into the cryptographic function. In response, he admitted that his patent failed to teach such a requirement of the claims in the '216 patent. (See Exhibit F Trial Transcript, p. 61:17 - p. 62:4.) The pertinent portion of the transcript is shown below for convenience as follows:

> [Attorney] Question: If you wanted to indicate that information associated with the user, unique information was input into the cryptographic function, you certainly had the ability to disclose that in the figures, if you so chose.
> [Hellman] Answer: Correct.
> [Attorney] Question: And you didn't?
> [Hellman] Answer: Correct.
> [Attorney] Question: And you also had the ability to describe in the patent, if you so chose?
> [Hellman] Answer: In the specification? Yes.
> [Attorney] Question: And you didn't?
> [Hellman] Answer: Correct

Uniloc's position is thus supported by Hellman himself.

See Office Action Response filed Mar. 18, 2011 at 11, 12, 14-15, 19-22, and 31-32.

See, e.g., id. at 11:

Regardless of the Office's application of its new construction of "licensee unique ID generating means," the Office has also factually mischaracterized Hellman with respect to that term. Contrary to the Office's interpretation, the BILLING INFORMATION is not associated with authorization A (or check value C). (*See*, Hellman FIG. 2; 6:16-30; 7:6-13; FIG. 7; and 10:14-32.) Nor is any user specific information input to Hellman's cryptographic function generators that generate A and C. (*Id.*) Indeed, Hellman explicitly states that authorization A is not associated with a user, but rather is base unit (*e.g.*, a personal computer) specific. (Hellman, 12:1-9.)

The Federal Circuit came to the same conclusion in a decision rendered two weeks prior to the Second Action when it considered whether the very same Hellman reference anticipated the very same claim limitation in an invalidity charge against the very same patent at issue here. The Federal Circuit stated:

> The "user billing information" in [Hellman] is not an input into the hash function and is thus irrelevant in determining whether [Hellman] discloses the "licensee unique ID" and "licensee unique ID generating means" elements of the '216 patent.

Uniloc USA, Inc. v. Microsoft Corp., --- F.3d ---, 2011 WL 9738, *56, n. 3 (Fed. Cir. 2011). While a court's decision that a patent is not invalid is generally not binding on the Office, the situation in this case is unusual. The Office ought to give deference to a Federal Circuit decision where it ruled on the same issue now before the central reexamination unit — whether Hellman anticipates claim 19 of the '216 patent. This is especially true where the claim terms at issue are drafted under § 112(6) and the Office must interpret this term in the same manner as the courts. *In re Donaldson*, 16 F.3d 1189, 1193 (Fed. Cir. 1994).

See, e.g., id. at 12:

Finally, the proposed modification to Hellman still does not address Hellman's main deficiency that it does not use any information uniquely associated with an intended licensee to generate its authorization A (or check value C). Thus, even with the proposed modification in view of Grundy, Hellman's system still does not generate the claimed "licensee unique ID," which as a matter of law is evidence that the invention is not obvious.

See, e.g., id. at 14-15:

Uniloc's consistent position, which as a matter of law has been confirmed by the Federal Circuit, is that the claimed "licensee unique ID" must be "a unique identifier associated with a licensee." *Uniloc v. Microsoft*, Case No. 03-440S, slip op. at 21 (D.R.I. 2006). To accomplish this, there must be some input to the means for generating the claimed "licensee unique ID" that characterizes the intended user. Hellman's cryptographic function generator has no such input and, as the Examiner correctly acknowledged (Second Action, p. 20), its output is solely descriptive of the licensee's computer. (*See*, Hellman, 6:16 - 7:2.) Therefore, even under a broadest reasonable interpretation standard, Hellman's cryptographic function generator does not (and cannot) anticipate the claimed "licensee unique ID generating means." Uniloc's interpretation is the more reasonable position and should be adopted by the Office as it was by the Federal Circuit.

See, e.g., id. at 19-22:

be, in the end, the correct construction"). The claim term on its face suggests that the ID be generated with some input that is unique to an intended licensee. The term "ID" is modified by the terms "licensee" and "unique." If those terms are to have any meaning in the § 112(6) context, they must carry some weight in the function ascribed to the generating means. That is, there must be some input to the generating means capable of making the resulting "licensee unique ID" uniquely associated with an intended licensee.

The specification is also clear in this regard—the "licensee unique ID" must be generated from some information that is unique to the intended licensee. (*See*, '216 patent, 2:65 - 3:2.) Every example in the specification of the '216 patent is consistent with that requirement. The "licensee unique ID" cannot be based on information that is solely representative of a base unit. (*Id.* at 1:66 - 2:7.) Indeed, such an interpretation is explicitly disclaimed in the Background of the '216 patent specification. ('216 patent, 1:60-65 and 2:4-7.) To generate a licensee unique ID, there must therefore be some input into the generating means that is uniquely associated with the intended licensee. Absent such input, the ID could not be uniquely associated with an intended licensee.

The Office has attempted to equate Hellman's cryptographic function generators 23 and 38 with the claimed "licensee unique ID generating means." (Second Action, p. 9.) But Hellman's cryptographic function generator receives no input that is uniquely associated with

the intended licensee. (Rosenblatt, ¶¶ 38-39.) Hellman's authorization A and check value C are limited to identification of the base unit or the platform on which the software is to be run. (Hellman, 12:5-8.) As noted above, such an ID was disclaimed in the Background of the '216 patent specification. Hellman's cryptographic function generators 23 and 38 therefore cannot perform the identical function as the claimed "licensee unique ID generating means" in the '216 patent.

That "BILLING INFORMATION" in Hellman is NOT associated with Hellman's authorization A or check value C is made explicitly clear by the Hellman reference itself. First, the billing information is not used to generate the authorization and check values (A and C, respectively) in Hellman. Inputs to cryptographic function generator 38 are limited to K (the cipher key), N (the number of desired software uses), R (a random number), and H (signal representing the software to be licensed).

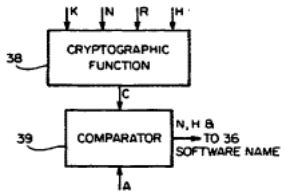


FIG_7

There is no input into Hellman's cryptographic function that is uniquely associated with an intended licensee. (Rosenblatt, ¶¶ 38-39.) This is indisputable and has been affirmed by the Federal Circuit.

Second, Hellman teaches that "authentication of the source of requests [*i.e.*, the intended licensee] is not required. However, it may be necessary to protect against one individual requesting software uses to be billed to another individual's account. Note that *the authorization would be of no use to the first individual since authorizations are base unit specific.*" (Hellman, 12:5-8; emphasis added.) In other words, Hellman teaches that base-unit-specific licensing of software is, in and of itself, sufficient to discourage unauthorized use obtained through fraudulent billing.

Hellman then proposes a solution to the fraudulent billing problem that STILL does not rely on any information unique to the user (such as billing information) in generating a unique ID. (Hellman, 12:10-26.) Any billing information in Hellman is thus used solely for payment, not for creating authorization A.

Third, Hellman's own testimony during the district court litigation also confirms Uniloc's position. (Exhibit A, A2723-45.)

> [Attorney] Question: If you wanted to indicate that information associated with the user, unique information was input into the cryptographic function, you certainly had the ability to disclose that in the figures, if you so chose.
> [Hellman] Answer: Correct.
> [Attorney] Question: And you didn't?
> [Hellman] Answer: Correct.
> [Attorney] Question: And you also had the ability to describe in the patent, if you so chose?
> [Hellman] Answer: In the specification? Yes.
> [Attorney] Question: And you didn't?
> [Hellman] Answer: Correct

(*Id.* at A2743.)

Hellman fails to teach a licensee unique ID generating means. For at least these reasons, Hellman does not anticipate independent claims 19 and 20. The Federal Circuit's decision affirming the District Court judgment on validity over Hellman is consistent with

Uniloc's position. The pending anticipation rejection of claims 19 and 20 should thus be reconsidered and withdrawn, consistent with the 2011 Federal Circuit decision.

See Declaration of William R. Rosenblatt Under 37 C.F.R. § 1.132, filed Nov. 29, 2010, ¶¶ 16-21, 23, 36-47, 66-68, 72-74, 80-83.

See, e.g., id. at ¶¶ 38-40:

38. First, regarding Hellman and "***licensee*** ID generation": the process in Hellman cited by the examiner above shows that the "check value C" (Hellman at 10:17), which the Examiner equates to LUID, is generated from four inputs, designated as K, N, R, and H. Of these: K is a ***key*** to a cryptographic function, which is an indicium of the ***computer*** on which the software is intended to be run. N is the ***number of usages*** of the software requested by the user (see Hellman at 5:65-66); R is a ***random number*** (Hellman at 5:66); H is an indicium of the ***software package*** being authorized for use (Hellman at 6:31-35), which is computed by means of a hash function. A hash function produces a value that serves as a mathematical "shorthand" for some data that has properties described appropriately in Hellman at 6:38-61, including that it is efficient to calculate and store.

39. None of these four inputs is an indicium of the ***licensee*** of the software, i.e., the user intending to run the software on the computer. Therefore Hellman does not teach "licensee ID generation."

40. I have reviewed Hellman's sworn testimony at trial. It reinforces my conclusion. The following is an excerpt from examination of Hellman at trial:

> [Attorney] Question: If you wanted to indicate that information associated with the user, unique information was input into the cryptographic function, you certainly had the ability to disclose that in the figures, if you so chose.
> [Hellman] Answer: Correct.
> [Attorney] Question: And you didn't?
> [Hellman] Answer: Correct.

[Attorney] Question: And you also had the ability to describe in the patent, if you so chose?
[Hellman] Answer: In the specification? Yes.
[Attorney] Question: And you didn't?
[Hellman] Answer: Correct.
(March 31, 2009 Trial Transcript: p. 61, ll 17 - p. 62, ll 4, Uniloc USA, Inc. et al. v. Microsoft Corp., C.A. No. 03-440 (D.R.I.))

See Notice of Intent to Issue Reexamination Certificate, mailed on Aug. 5, 2011 at 5:

that decision. The Patent Owner has persuasively argued that, based on such decisions regarding the '216 patent, Hellman cannot be reasonably construed as teaching to a local licensee unique ID generating means or a remote licensee unique ID generating means.

The licensee unique ID generated by the means recited in each of the claims must be derived from at least piece of information that is specific to the user, such as name, billing information, or product information unique to the instantiation entered by the user. The information cannot be specific to the computer or independently generated by the computer. Hellman's ID has four inputs: a computer-specific key (SK), a number of uses requested (N), a random number generated by the computer (R), and a hash of a code for the type of software package, which is general to all installations of that package (H). Since none of these are user-specific, Hellman's algorithm does not generated the claimed licensee unique ID.

Defendants may rely on other statements made by Uniloc during the reexamination, as well other specific statements made by the declarants in the declarations submitted by Uniloc during the reexamination. In addition, Defendants note that Uniloc has just produced, on August 29, 2011, the lengthy declaration of William Rosenblatt. While Defendants have cited to certain portions of that declaration, above, Defendants reserve the right to rely on other portions of that declaration, which appears to include extensive support for the disclaimer.