

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

**MARKING OBJECT VIRTUALIZATION
INTELLIGENCE, LLC,**

Plaintiff,

v.

CISCO SYSTEMS, INC.

Defendant.

Civil Action No. 2:16-cv-1040

JURY TRIAL DEMANDED

AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Marking Object Virtualization Intelligence, LLC (“MOV Intelligence” or “Plaintiff”), by and through its attorneys, brings this action and makes the following allegations of patent infringement relating to U.S. Patent Nos.: 7,200,230 (“the ‘230 patent”); 6,802,006 (“the ‘006 patent”); 6,510,516 (“the ‘516 patent”); 7,650,504 (“the ‘504 patent”); 7,650,418 (“the ‘418 patent”); 7,124,114 (“the ‘114 patent”); and 6,813,640 (“the ‘640 patent”) (collectively, the “patents-in-suit” or the “MOV Intelligence Patents”). Defendant Cisco Systems, Inc. (“Cisco” or “Defendant”) infringes each of the patents-in-suit in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq.*

THE PARTIES

MARKING OBJECT VIRTUALIZATION INTELLIGENCE, LLC

1. Marking Object Virtualization Intelligence, LLC (“MOV Intelligence”) is a Texas limited liability company with its principal place of business located at 903 East 18th Street, Suite 217, Plano, Texas 75074. MOV Intelligence is committed to advancing the current state of DRM and watermarking technologies.

2. MOV Intelligence Global Licensing, LLC (“MOV Global Licensing”) is a wholly-owned subsidiary of MOV Intelligence and assists in the licensing of MOV Intelligence’s patents in territories outside the United States with a focus on the European Union (and the

United Kingdom). MOV Intelligence Global Licensing, LLC is a corporation organized under the laws of Delaware.

CISCO SYSTEMS, INC.

3. On information and belief, Cisco Systems, Inc. is a California corporation with its principal place of business at 170 West Tasman Drive, San Jose, California 95134. Cisco may be served through its registered agent Prentice Hall Corporation System, 211 E. 7th Street, Suite 620, Austin, Texas 78701. On information and belief, Cisco is registered to do business in the State of Texas, and has been since at least December 29, 1989.

4. On information and belief, Cisco conducts business operations within the Eastern District of Texas in its facilities at 2200 E. President George Bush Highway, Richardson, Texas 75082.

JURISDICTION AND VENUE

5. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

6. Upon information and belief, this Court has personal jurisdiction over Cisco in this action because Cisco has committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Cisco would not offend traditional notions of fair play and substantial justice. Cisco, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit. In addition, Defendant Cisco is registered to do business in the State of Texas.

7. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Cisco is registered to do business in Texas, and upon information and belief, has transacted business in the Eastern District of Texas and has committed acts of direct and indirect infringement in the

Eastern District of Texas. Plaintiff MOV Intelligence is not owned or controlled by Rovi Corporation or any affiliate of Rovi Corporation.

THE ASSERTED PATENTS

U.S. PATENT NO. 7,200,230

8. U.S. Patent No. 7,200,230 (the “230 patent”), entitled “System and Method for Controlling and Enforcing Access Rights to Encrypted Media,” was filed January 15, 2001, and claims priority to April 6, 2000. MOV Intelligence is the owner by assignment of all right, title, and interest in the ‘230 patent. A true and correct copy of the ‘230 patent is attached hereto as Exhibit A.

U.S. PATENT NO. 6,802,006

9. U.S. Patent No. 6,802,006 (the “’006 patent”), entitled System and Method of Verifying the Authenticity of Dynamically Connectable Executable Images, was filed on July 22, 1999, and claims priority to January 15, 1999. MOV Intelligence is the owner by assignment of all right, title, and interest in the ‘006 patent. A true and correct copy of the ‘006 patent is attached hereto as Exhibit B.

U.S. PATENT NO. 6,510,516

10. U.S. Patent No. 6,510,516 (the “’516 patent”), entitled System and Method for Authenticating Peer Components, was filed on January 15, 1999, and claims priority to January 16, 1998. MOV Intelligence is the owner by assignment of all right, title, and interest in the ‘516 patent. A true and correct copy of the ‘516 patent is attached hereto as Exhibit C.

U.S. PATENT NO. 7,650,504

11. U.S. Patent No. 7,650,504 (the “’504 patent”), entitled “System and Method of Verifying the Authenticity of Dynamically Connectable Executable Images,” was filed on August 23, 2004, and claims priority to July 22, 1999. MOV Intelligence is the owner by assignment of all right, title, and interest in the ‘504 patent. A true and correct copy of the ‘504 patent is attached hereto as Exhibit D.

U.S. PATENT NO. 7,650,418

12. U.S. Patent No. 7,650,418 (the “‘418 patent”), entitled “System and Method for Controlling the Usage of Digital Objects,” was filed on August 26, 2004, and claims priority to December 8, 1998. MOV Intelligence is the owner by assignment of all right, title, and interest in the ‘418 patent. A true and correct copy of the ‘418 patent is attached hereto as Exhibit E.

U.S. PATENT NO. 7,124,114

13. U.S. Patent No. 7,124,114 (the “‘114 patent”), entitled “Method and Apparatus for Determining Digital A/V Content Distribution Terms Based on Detected Piracy Levels,” was filed on November 9, 2000. MOV Intelligence is the owner by assignment of all right, title, and interest in the ‘114 patent. A true and correct copy of the ‘114 patent is attached hereto as Exhibit F.

U.S. PATENT NO. 6,813,640

14. U.S. Patent No. 6,813,640 (the “‘640 patent”), entitled “System and Method for Controlling the Editing by User Action of Digital Objects Created in a Document Server Application,” was filed on July 21, 2000, and claims priority to December 8, 1998. MOV Intelligence is the owner by assignment of all right, title, and interest in the ‘640 patent. A true and correct copy of the ‘640 patent is attached hereto as Exhibit G.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 7,200,230

15. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

16. Cisco designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for digital rights management.

17. Cisco designs, makes, sells, offers to sell, imports, and/or uses Cisco Identity Services Engine Release Nos. 1.0.4, 1.1, 1.2, 1.3, 1.4, 2.0, and 2.1 (the “Cisco ‘230 Products”).

18. On information and belief, one or more Cisco subsidiaries and/or affiliates use the Cisco ‘230 Products in regular business operations.

19. On information and belief, one or more of the Cisco '230 Products include digital rights management technology.

20. On information and belief, one or more of the Cisco '230 Products enable associating a user program key with a user program configured to run on a user data processor.

21. On information and belief, the Cisco '230 Products are available to businesses and individuals throughout the United States.

22. On information and belief, the Cisco '230 Products are provided to businesses and individuals located in the Eastern District of Texas.

23. On information and belief, the Cisco '230 Products enable determining whether the use of the data object is to be restricted to a particular user data processor.

24. On information and belief, the Cisco '230 Products comprise a system wherein a machine key device is associated with the particular user data processor. Further, the machine key device is accessible by the user program, and the machine key device maintains a portion of a machine key.

25. On information and belief, the Cisco '230 Products enable encrypting a data object so the decryption of a first secure layer and a second secure layer of the encrypted data object requires the user program key and the machine key.

26. On information and belief, the Cisco '230 Products enable determining whether the use of the data object is to be restricted to a particular user.

27. On information and belief, the Cisco '230 Products provide for the designation and authentication of the identity of a user by whom the data object is to be used.

28. On information and belief, the Cisco '230 Products enable associating a user key device with the particular user. Further, the Cisco '230 Products enable the user key device to be made accessible by the user program. And, the user key device maintains a portion of a user key.

29. On information and belief, the Cisco '230 Products contain functionality for encrypting a data object so the decryption of a third secure layer of the encrypted data object requires the user key.

30. On information and belief, the Cisco '230 Products contain functionality wherein the third key used by the system for managing digital rights is the media access controller (MAC) address of the user data processor.

31. On information and belief, the Cisco '230 Products provide for encryption of a data object so only a designated data processor can decrypt and use the data object.

32. On information and belief, the Cisco '230 Products enable user specific digital rights management authorization and access.

33. On information and belief, Cisco has directly infringed and continues to directly infringe the '230 patent by, among other things, making, using, offering for sale, and/or selling digital content protection technology, including but not limited to the Cisco '230 Products, which include infringing digital rights management technology. Such products and/or services include, by way of example and without limitation, the Cisco Identity Services Engine Release Nos. 1.0.4, 1.1, 1.2, 1.3, 1.4, 2.0, and 2.1.

34. By making, using, testing, offering for sale, and/or selling digital rights management products and services, including but not limited to the Cisco '230 Products, Cisco has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '230 patent, including at least claim 39, pursuant to 35 U.S.C. § 271(a).

35. On information and belief, Cisco also indirectly infringes the '230 patent by actively inducing infringement under 35 USC § 271(b).

36. On information and belief, Cisco had knowledge of the '230 patent since at least November 2014, when U.S. Patent No. 8,312,265 was assigned to Cisco. U.S. Patent No. 8,312,265 cites WO2001078285, which is the World Intellectual Property Organization ("WIPO") counterpart to the '230 patent. Alternatively, Cisco had knowledge of the '230 patent since at least 2014 when WIPO App. No. 2003/050,996, which cites the WIPO counterpart to the

‘230 patent (WO2001078285), was assigned to Cisco. Alternatively, Cisco had knowledge of the ‘230 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Cisco knew of the ‘230 patent and knew of its infringement, including by way of this lawsuit.

37. On information and belief, Cisco intended to induce patent infringement by third-party customers and users of the Cisco ‘230 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Cisco specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘230 patent. Cisco performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the ‘230 patent and with the knowledge that the induced acts would constitute infringement. For example, Cisco provides the Cisco ‘230 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘230 patent, including at least claim 39, and Cisco further provides documentation and training materials that cause customers and end users of the Cisco ‘230 Products to utilize the products in a manner that directly infringe one or more claims of the ‘230 patent. By providing instruction and training to customers and end-users on how to use the Cisco ‘230 Products in a manner that directly infringes one or more claims of the ‘230 patent, including at least claim 39, Cisco specifically intended to induce infringement of the ‘230 patent. On information and belief, Cisco engaged in such inducement to promote the sales of the Cisco ‘230 Products, e.g., through Cisco user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘230 patent. Accordingly, Cisco has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the ‘230 patent, knowing that such use constitutes infringement of the ‘230 patent.

38. The ‘230 patent is well-known within the industry as demonstrated by the over 180 citations to the ‘230 patent family in published patents and published patent applications assigned to technology companies and academic institutions. Moreover, Cisco had knowledge of

the '230 patent since at least November 2014, when U.S. Patent No. 8,312,265 was assigned to Cisco. U.S. Patent No. 8,312,265 cites WO2001078285, which is the World Intellectual Property Organization ("WIPO") counterpart to the '230 patent. Alternatively, Cisco had knowledge of the '230 patent since at least 2014 when WIPO App. No. 2003/050,996, which cites the WIPO counterpart to the '230 patent (WO2001078285), was assigned to Cisco. Several of Cisco's competitors have paid considerable licensing fees for their use of the technology claimed by the '230 patent. In an effort to gain an advantage over Cisco's competitors by utilizing the same licensed technology without paying reasonable royalties, Cisco infringed the '230 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

39. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '230 patent.

40. As a result of Cisco's infringement of the '230 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Cisco's infringement, but in no event less than a reasonable royalty for the use made of the invention by Cisco together with interest and costs as fixed by the Court.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 6,802,006

41. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

42. Cisco designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for determining the authenticity of an executable image.

43. Cisco designs, makes, sells, offers to sell, imports, and/or uses Cisco IOS Release Nos. 15.5M&T, 15.4S, 15.4M&T, 15.3S, 15.3M&T, 15.2S, 15.2M&T, 15.1M&T, 15.1S, 15.1SY, 15.0M, 15.0S, 15.0SY (the "Cisco '006 Products").

44. On information and belief, one or more Cisco subsidiaries and/or affiliates use the Cisco '006 Products in regular business operations.

45. On information and belief, one or more of the Cisco '006 Products include authentication technology.

46. On information and belief, one or more of the Cisco '006 Products enable authenticating the identity of a software application in a dynamic loading environment. In particular, the Cisco '006 Products determine whether an executable image has been dynamically connected to another data object that has been tampered with subsequent to the execution of the software application.

47. On information and belief, the Cisco '006 Products are available to businesses and individuals throughout the United States.

48. On information and belief, the Cisco '006 Products are provided to businesses and individuals located in the Eastern District of Texas.

49. On information and belief, the Cisco '006 Products enable identifying one or more locations within the executable image, each of the identified locations being modified by a program loader.

50. On information and belief, the Cisco '006 Products comprise a system wherein a reference digital signature is generated based on an executable image.

51. On information and belief, the Cisco '006 Products generate a reference digital signature that excludes one or more locations in an executable image.

52. On information and belief, the Cisco '006 Products are capable of storing the reference digital signature on a computer network.

53. On information and belief, the Cisco '006 Products comprise systems and methods wherein an authenticity digital signature is generated based on an executable image.

54. On information and belief, the Cisco '006 Products comprise systems and methods that generate an authenticity digital signature that excludes one or more locations in an executable image.

55. On information and belief, the Cisco '006 Products comprise systems and methods that determine whether the authenticity digital signature matches the reference digital signature.

56. On information and belief, the Cisco '006 Products contain functionality that generates a warning if the reference digital signature does not match the authenticity digital signature.

57. On information and belief, the Cisco '006 Products contain functionality wherein the digital signature is generated based on a first and second point in time. For example, one or more of the Cisco '006 Products generate a reference digital signature at a first point in time. Subsequently, an authenticity digital signature is generated (at a second point in time).

58. On information and belief, the Cisco '006 Products comprise a system and method that generates a digital signature based on a hash value. Specifically, the reference digital signature that is generated by the Cisco '006 Products at a first point in time is based on a hash value. Later the authenticity digital signature is also generated based on a hash function that is used to check data integrity.

59. On information and belief, the Cisco '006 Products comprise a system and method that can verify the identity a computer application.

60. On information and belief, the Cisco '006 Products enable the detection of corrupted data in a computer image.

61. On information and belief, the Cisco '006 Products enable the verification of the integrity of software images.

62. On information and belief, Cisco has directly infringed and continues to directly infringe the '006 patent by, among other things, making, using, offering for sale, and/or selling content protection technology, including but not limited to the Cisco '006 Products, which includes technology for verifying the authenticity of a software image. Such products and/or services include, by way of example and without limitation, the Cisco IOS Release Nos.

15.5M&T, 15.4S, 15.4M&T, 15.3S, 15.3M&T, 15.2S, 15.2M&T, 15.1M&T, 15.1S, 15.1SY, 15.0M, 15.0S, 15.0SY.

63. By making, using, testing, offering for sale, and/or selling verification and authentication products and services, including but not limited to the Cisco '006 Products, Cisco has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '006 patent, including at least claims 1, 3, 14, and 15, pursuant to 35 U.S.C. § 271(a).

64. On information and belief, Cisco also indirectly infringes the '006 patent by actively inducing infringement under 35 USC § 271(b).

65. On information and belief, Cisco had knowledge of the '006 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Cisco knew of the '006 patent and knew of its infringement, including by way of this lawsuit.

66. On information and belief, Cisco intended to induce patent infringement by third-party customers and users of the Cisco '006 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Cisco specifically intended and was aware that the normal and customary use of the accused products would infringe the '006 patent. Cisco performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '006 patent and with the knowledge that the induced acts would constitute infringement. For example, Cisco provides the Cisco '006 Products that have the capability of operating in a manner that infringe one or more of the claims of the '006 patent, including at least claims 1, 3, 14, and 15, and Cisco further provides documentation and training materials that cause customers and end users of the Cisco '006 Products to utilize the products in a manner that directly infringe one or more claims of the '006 patent. By providing instruction and training to customers and end-users on how to use the Cisco '006 Products in a manner that directly infringes one or more claims of the '006 patent, including at least claims 1, 3, 14, and 15, Cisco specifically intended to induce infringement of the '006 patent. On information and belief, Cisco

engaged in such inducement to promote the sales of the Cisco '006 Products, *e.g.*, through Cisco user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '006 patent. Accordingly, Cisco has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '006 patent, knowing that such use constitutes infringement of the '006 patent.

67. The '006 patent is well-known within the industry as demonstrated by the over 85 citations to the '006 patent in issued patents and published patent applications assigned to technology companies and academic institutions. Several of Cisco's competitors have paid considerable licensing fees for their use of the technology claimed by the '006 patent. In an effort to gain an advantage over Cisco's competitors by utilizing the same licensed technology without paying reasonable royalties, Cisco infringed the '006 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

68. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '006 patent.

69. As a result of Cisco's infringement of the '006 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Cisco's infringement, but in no event less than a reasonable royalty for the use made of the invention by Cisco together with interest and costs as fixed by the Court.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 6,510,516

70. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

71. Cisco designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for authenticating peer data objects.

72. Cisco designs, makes, sells, offers to sell, imports, and/or uses Cisco Identity Services Engine Release Nos. 1.0.4, 1.1, 1.2, 1.3, 1.4, 2.0, and 2.1 (the “Cisco ‘516 Products”).

73. On information and belief, one or more Cisco subsidiaries and/or affiliates use the Cisco ‘516 Products in regular business operations.

74. On information and belief, one or more of the Cisco ‘516 Products include authentication technology.

75. On information and belief, one or more of the Cisco ‘516 Products enable authenticating the identity of peers to a data object.

76. On information and belief, the Cisco ‘516 Products are available to businesses and individuals throughout the United States.

77. On information and belief, the Cisco ‘516 Products are provided to businesses and individuals located in the Eastern District of Texas.

78. On information and belief, the Cisco ‘516 Products enable first data objects to contain or be linked to a description of one or more peer data objects that are required to be connected to the first data object before the data object can be accessed by the peer data objects.

79. On information and belief, the Cisco ‘516 Products enable the use of a digital signature that identifies the provider of a data object.

80. On information and belief, the Cisco ‘516 Products contain systems and methods that comprise reading from a data object a description of one or more peer data objects that is required for use of the data object.

81. On information and belief, the Cisco ‘516 Products contain functionality for determining whether the data object is authorized to communicate with one or more peer data objects.

82. On information and belief, the Cisco ‘516 Products contain the capability to determine if the data object is authorized to communicate with one or more peer data objects.

83. On information and belief, the Cisco ‘516 Products are capable of controlling the connection of the peer data objects to the data object.

84. On information and belief, the Cisco '516 Products comprise systems and methods that connect a data object to peer data objects based upon authorization being granted. Moreover, when authorization is granted for the connection of a data object to peer data objects the peer data objects can communicate with the data object and the data object can communicate with the peer data objects.

85. On information and belief, the Cisco '516 Products support authenticating a data object where the data object is encrypted.

86. On information and belief, Cisco has directly infringed and continues to directly infringe the '516 patent by, among other things, making, using, offering for sale, and/or selling data object authentication and verification technology, including but not limited to the Cisco '516 Products, which include infringing verification and authentication technologies. Such products and/or services include, by way of example and without limitation, the Cisco Identity Services Engine Release Nos. 1.0.4, 1.1, 1.2, 1.3, 1.4, 2.0, and 2.1.

87. By making, using, testing, offering for sale, and/or selling authentication and verification products and services, including but not limited to the Cisco '516 Products, Cisco has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '516 patent, including at least claims 1, 17, and 20, pursuant to 35 U.S.C. § 271(a).

88. On information and belief, Cisco also indirectly infringes the '516 patent by actively inducing infringement under 35 USC § 271(b).

89. On information and belief, Cisco had knowledge of the '516 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Cisco knew of the '516 patent and knew of its infringement, including by way of this lawsuit.

90. On information and belief, Cisco intended to induce patent infringement by third-party customers and users of the Cisco '516 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Cisco specifically intended and was aware that the normal and customary

use of the accused products would infringe the '516 patent. Cisco performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '516 patent and with the knowledge that the induced acts would constitute infringement. For example, Cisco provides the Cisco '516 Products that have the capability of operating in a manner that infringe one or more of the claims of the '516 patent, including at least claims 1, 17, and 20, and Cisco further provides documentation and training materials that cause customers and end users of the Cisco '516 Products to utilize the products in a manner that directly infringe one or more claims of the '516 patent. By providing instruction and training to customers and end-users on how to use the Cisco '516 Products in a manner that directly infringes one or more claims of the '516 patent, including at least claims 1, 17, and 20, Cisco specifically intended to induce infringement of the '516 patent. On information and belief, Cisco engaged in such inducement to promote the sales of the Cisco '516 Products, e.g., through Cisco user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '516 patent. Accordingly, Cisco has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '516 patent, knowing that such use constitutes infringement of the '516 patent.

91. The '516 patent is well-known within the industry as demonstrated by the over 108 citations to the '516 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (e.g., LG Electronics, Inc. and Siemens AG). Several of Cisco's competitors have paid considerable licensing fees for their use of the technology claimed by the '516 patent. In an effort to gain an advantage over Cisco's competitors by utilizing the same licensed technology without paying reasonable royalties, Cisco infringed the '516 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

92. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '516 patent.

93. As a result of Cisco's infringement of the '516 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Cisco's infringement, but in no event less than a reasonable royalty for the use made of the invention by Cisco together with interest and costs as fixed by the Court.

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 7,650,504

94. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

95. Cisco designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for verifying the authenticity of executable images.

96. Cisco designs, makes, sells, offers to sell, imports, and/or uses Cisco IOS Release Nos. 15.5M&T, 15.4S, 15.4M&T, 15.3S, 15.3M&T, 15.2S, 15.2M&T, 15.1M&T, 15.1S, 15.1SY, 15.0M, 15.0S, 15.0SY (the "Cisco '504 Products").

97. On information and belief, one or more Cisco subsidiaries and/or affiliates use the Cisco '504 Products in regular business operations.

98. On information and belief, one or more of the Cisco '504 Products include authentication technology.

99. On information and belief, one or more of the Cisco '504 Products comprise systems and methods for determining the authenticity of an executable image.

100. On information and belief, one or more of the Cisco '504 Products enable authenticating and verifying an executable image. In particular, the Cisco '504 Products determine whether a software application that has been dynamically connected to another data object has been tampered with subsequent to the execution of the software application.

101. On information and belief, the Cisco '504 Products are available to businesses and individuals throughout the United States.

102. On information and belief, the Cisco '504 Products are provided to businesses and individuals located in the Eastern District of Texas.

103. On information and belief, the Cisco '504 Products enable the use of a reference digital signature for an executable image. The reference digital signature uses the contents of the executable image excluding portions of the executable that are fixed-up by a program loader.

104. On information and belief, the Cisco '504 Products comprise a system wherein a reference digital signature is generated based on an executable image.

105. On information and belief, the Cisco '504 Products generate a reference digital signature that excludes one or more locations in an executable image.

106. On information and belief, the Cisco '504 Products comprise systems and methods wherein subsequent to the loading of the executable image the '504 Products determine an authenticity digital signature to verify that the executable image has not been improperly modified.

107. On information and belief, the Cisco '504 Products comprise systems and methods that generate an authenticity digital signature that excludes one or more locations in an executable image.

108. On information and belief, the Cisco '504 Products are systems and methods that generate an authenticity digital signature after the executable image is loaded into memory. The authenticity digital signature which is generated by the Cisco '504 Products excludes one or more pointers in need of fixing up;

109. On information and belief, the Cisco '504 Products comprise systems and methods that determine whether the authenticity digital signature matches the reference digital signature.

110. On information and belief, the Cisco '504 Products enable the generating of a reference digital signature prior to loading the executable image into memory. Specifically, the Cisco '504 Products generate a reference digital signature that excludes one or more pointers from the reference digital signature.

111. On information and belief, the Cisco '504 Products contain functionality wherein the digital signature is generated based on a first and second point in time.

112. On information and belief, the Cisco '504 Products have the ability to compare the reference digital signature and the authenticity digital signature to perform an authenticity check.

113. On information and belief, the Cisco '504 Products enable the detection of corrupted data in a computer image.

114. On information and belief, the Cisco '504 Products enable the verification of the integrity of software images.

115. On information and belief, Cisco has directly infringed and continues to directly infringe the '504 patent by, among other things, making, using, offering for sale, and/or selling content protection technology, including but not limited to the Cisco '504 Products, which includes technology for verifying the authenticity of a software image. Such products and/or services include, by way of example and without limitation, the Cisco IOS Release Nos. 15.5M&T, 15.4S, 15.4M&T, 15.3S, 15.3M&T, 15.2S, 15.2M&T, 15.1M&T, 15.1S, 15.1SY, 15.0M, 15.0S, 15.0SY.

116. By making, using, testing, offering for sale, and/or selling authentication and verification technologies and services, including but not limited to the Cisco '504 Products, Cisco has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '504 patent, including at least claims 1 and 10, pursuant to 35 U.S.C. § 271(a).

117. On information and belief, Cisco also indirectly infringes the '504 patent by actively inducing infringement under 35 USC § 271(b).

118. On information and belief, Cisco had knowledge of the '504 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Cisco knew of the '504 patent and knew of its infringement, including by way of this lawsuit.

119. On information and belief, Cisco intended to induce patent infringement by third-party customers and users of the Cisco '504 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Cisco specifically intended and was aware that the normal and customary use of the accused products would infringe the '504 patent. Cisco performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '504 patent and with the knowledge that the induced acts would constitute infringement. For example, Cisco provides the Cisco '504 Products that have the capability of operating in a manner that infringe one or more of the claims of the '504 patent, including at least claims 1 and 10, and Cisco further provides documentation and training materials that cause customers and end users of the Cisco '504 Products to utilize the products in a manner that directly infringe one or more claims of the '504 patent. By providing instruction and training to customers and end-users on how to use the Cisco '504 Products in a manner that directly infringes one or more claims of the '504 patent, including at least claims 1 and 10, Cisco specifically intended to induce infringement of the '504 patent. On information and belief, Cisco engaged in such inducement to promote the sales of the Cisco '504 Products, e.g., through Cisco user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '504 patent. Accordingly, Cisco has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '504 patent, knowing that such use constitutes infringement of the '504 patent.

120. The '504 patent is well-known within the industry as demonstrated by the over 30 citations to the '504 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Apple, Inc. and Electronics and Telecommunications Research Institute (ETRI)). Several of Cisco's competitors have paid considerable licensing fees for their use of the technology claimed by the '504 patent. In an effort to gain an advantage over Cisco's competitors by utilizing the same licensed technology

without paying reasonable royalties, Cisco infringed the '504 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

121. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '504 patent.

122. As a result of Cisco's infringement of the '504 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Cisco's infringement, but in no event less than a reasonable royalty for the use made of the invention by Cisco together with interest and costs as fixed by the Court.

COUNT V
INFRINGEMENT OF U.S. PATENT NO. 7,650,418

123. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

124. Cisco designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for controlling the usage of digital objects.

125. Cisco designs, makes, sells, offers to sell, imports, and/or uses the Cisco Wide Area Application Versions 4.2.1 and later (the "Cisco '418 Products").

126. On information and belief, one or more Cisco subsidiaries and/or affiliates use the Cisco '418 Products in regular business operations.

127. On information and belief, one or more of the Cisco '418 Products comprise systems and methods for intercepting a communication between two applications in a computer environment.

128. On information and belief, one or more of the Cisco '418 Products enable intercepting a communication between two applications where the first and second application communicate via a predefined communications channel.

129. On information and belief, the Cisco '418 Products are available to businesses and individuals throughout the United States.

130. On information and belief, the Cisco '418 Products are provided to businesses and individuals located in the Eastern District of Texas.

131. On information and belief, the Cisco '418 Products include systems and methods that comprise a discreet intercept technology component (DIT) and a dynamic connection logic component (DCL).

132. On information and belief, the Cisco '418 Products comprise systems and methods wherein the DIT component permits the interception of communication and data flows between two or more components in component-based applications.

133. On information and belief, the Cisco '418 Products enable the DIT component to be inserted between two digital components. The DIT then intercepts the data and communications, thereby controlling the communication between the two digital components.

134. On information and belief, the Cisco '418 Products comprise systems and methods that enable a control object capable of specifying a dynamic control logic depending on the intercepted data communication.

135. On information and belief, the Cisco '418 Products enable applying by the intercept application the dynamic control logic specified by the control object on the digital object.

136. On information and belief, the Cisco '418 Products contain functionality for intercepting data communication between a first application and a second application within a computer network without changing the functionality of the first application and the second application.

137. On information and belief, Cisco has directly infringed and continues to directly infringe the '418 patent by, among other things, making, using, offering for sale, and/or selling digital rights technology, including but not limited to the Cisco '418 Products, which include infringing technology for controlling the usage of data objects. Such products and/or services

include, by way of example and without limitation, the Cisco Wide Area Application Versions 4.2.1 and later.

138. By making, using, testing, offering for sale, and/or selling digital rights management products and services, including but not limited to the Cisco '418 Products, Cisco has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '418 patent, including at least claims 1, 2, 4, 7, 8, and 9, pursuant to 35 U.S.C. § 271(a).

139. On information and belief, Cisco also indirectly infringes the '418 patent by actively inducing infringement under 35 USC § 271(b).

140. On information and belief, Cisco had knowledge of the '418 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Cisco knew of the '418 patent and knew of its infringement, including by way of this lawsuit.

141. On information and belief, Cisco intended to induce patent infringement by third-party customers and users of the Cisco '418 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Cisco specifically intended and was aware that the normal and customary use of the accused products would infringe the '418 patent. Cisco performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '418 patent and with the knowledge that the induced acts would constitute infringement. For example, Cisco provides the Cisco '418 Products that have the capability of operating in a manner that infringe one or more of the claims of the '418 patent, including at least claims 1, 2, 4, 7, 8, and 9, and Cisco further provides documentation and training materials that cause customers and end users of the Cisco '418 Products to utilize the products in a manner that directly infringe one or more claims of the '418 patent. By providing instruction and training to customers and end-users on how to use the Cisco '418 Products in a manner that directly infringes one or more claims of the '418 patent, including at least claims 1, 2, 4, 7, 8, and 9, Cisco specifically intended to induce infringement of the '418 patent. On information and belief,

Cisco engaged in such inducement to promote the sales of the Cisco '418 Products, e.g., through Cisco user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '418 patent. Accordingly, Cisco has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '418 patent, knowing that such use constitutes infringement of the '418 patent.

142. The '418 patent is well-known within the industry as demonstrated by the over 47 citations to the '418 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Google, Inc. and International Business Machines Corporation). Several of Cisco's competitors have paid considerable licensing fees for their use of the technology claimed by the '418 patent. In an effort to gain an advantage over Cisco's competitors by utilizing the same licensed technology without paying reasonable royalties, Cisco infringed the '418 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

143. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '418 patent.

144. As a result of Cisco's infringement of the '418 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Cisco's infringement, but in no event less than a reasonable royalty for the use made of the invention by Cisco together with interest and costs as fixed by the Court.

COUNT VI
INFRINGEMENT OF U.S. PATENT NO. 7,124,114

145. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

146. Cisco designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for managing the distribution of digital content and preventing unauthorized access to protected digital content.

147. Cisco designs, makes, sells, offers to sell, imports, and/or uses the Cisco FireSIGHT System Versions 5.3 and 5.4 and the Cisco Firepower System Version 6 (the “Cisco ‘114 Products”).

148. On information and belief, one or more Cisco subsidiaries and/or affiliates use the Cisco ‘114 Products in regular business operations.

149. On information and belief, one or more of the Cisco ‘114 Products include content protection and content access technology.

150. On information and belief, one or more of the Cisco ‘114 Products enable providing or withholding access to digital content in accordance with digital rights management protection terms.

151. On information and belief, the Cisco ‘114 Products are available to businesses and individuals throughout the United States.

152. On information and belief, the Cisco ‘114 Products are provided to businesses and individuals located in the Eastern District of Texas.

153. On information and belief, the Cisco ‘114 Products enable the distribution of protected digital data.

154. On information and belief, the Cisco ‘114 Products comprise systems and methods wherein the Cisco ‘114 Products ascertain terms for providing protected data to a prospective requestor according at least in part to information of unauthorized copying of other protected material previously provided to said prospective requestor.

155. On information and belief, the Cisco ‘114 Products comprise systems and methods that provide authorization to allow access or deny access to protected digital data based on ascertained terms.

156. On information and belief, Cisco has directly infringed and continues to directly infringe the '114 patent by, among other things, making, using, offering for sale, and/or selling digital content protection technology, including but not limited to the Cisco '114 Products, which include infringing digital rights management technologies. Such products and/or services include, by way of example and without limitation, the Cisco FireSIGHT System Versions 5.3 and 5.4 and the Cisco Firepower System Version 6.

157. By making, using, testing, offering for sale, and/or selling digital rights management and access control products and services, including but not limited to the Cisco '114 Products, Cisco has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '114 patent, including at least claims 1, 21, 41, and 52, pursuant to 35 U.S.C. § 271(a).

158. On information and belief, Cisco also indirectly infringes the '114 patent by actively inducing infringement under 35 USC § 271(b).

159. On information and belief, Cisco had knowledge of the '114 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Cisco knew of the '114 patent and knew of its infringement, including by way of this lawsuit.

160. On information and belief, Cisco intended to induce patent infringement by third-party customers and users of the Cisco '114 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Cisco specifically intended and was aware that the normal and customary use of the accused products would infringe the '114 patent. Cisco performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '114 patent and with the knowledge that the induced acts would constitute infringement. For example, Cisco provides the Cisco '114 Products that have the capability of operating in a manner that infringe one or more of the claims of the '114 patent, including at least claims 1, 21, 41, and 52, and Cisco further provides documentation and training materials that cause customers and end users of the Cisco '114 Products to utilize the products in a manner that

directly infringe one or more claims of the '114 patent. By providing instruction and training to customers and end-users on how to use the Cisco '114 Products in a manner that directly infringes one or more claims of the '114 patent, including at least claims 1, 21, 41, and 52, Cisco specifically intended to induce infringement of the '114 patent. On information and belief, Cisco engaged in such inducement to promote the sales of the Cisco '114 Products, e.g., through Cisco user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '114 patent. Accordingly, Cisco has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '114 patent, knowing that such use constitutes infringement of the '114 patent.

161. The '114 patent is well-known within the industry as demonstrated by the over 39 citations to the '114 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Aigo Research Institute of Image Computing Co., Ltd. and General Electric Company). Several of Cisco's competitors have paid considerable licensing fees for their use of the technology claimed by the '114 patent. In an effort to gain an advantage over Cisco's competitors by utilizing the same licensed technology without paying reasonable royalties, Cisco infringed the '114 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

162. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '114 patent.

163. As a result of Cisco's infringement of the '114 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Cisco's infringement, but in no event less than a reasonable royalty for the use made of the invention by Cisco together with interest and costs as fixed by the Court.

COUNT VII
INFRINGEMENT OF U.S. PATENT NO. 6,813,640

164. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

165. Cisco designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for controlling digital objects created in a document server application.

166. Cisco designs, makes, sells, offers to sell, imports, and/or uses the Cisco Cloud Object Storage Release versions 2.2.1, 2.1.2, 3.0.1, 3.5.1, and 3.5.2 (the “Cisco ‘640 Products”).

167. On information and belief, one or more Cisco subsidiaries and/or affiliates use the Cisco ‘640 Products in regular business operations.

168. On information and belief, one or more of the Cisco ‘640 Products comprise systems and methods for intercepting a communication between two applications in a computer environment.

169. On information and belief, one or more of the Cisco ‘640 Products enable intercepting a communication between two applications where the first and second application communicate via a predefined communications channel.

170. On information and belief, the Cisco ‘640 Products are available to businesses and individuals throughout the United States.

171. On information and belief, the Cisco ‘640 Products are provided to businesses and individuals located in the Eastern District of Texas.

172. On information and belief, the Cisco ‘640 Products include systems and methods that comprise a discreet intercept technology component (DIT) and a dynamic connection logic component (DCL).

173. On information and belief, the Cisco ‘640 Products comprise systems and methods wherein the DIT component permits the interception of communication and data flows between two or more components in component-based applications.

174. On information and belief, the Cisco '640 Products enable the DIT component to be inserted between two digital components. The DIT then intercepts the data and communications, thereby controlling the communication between the two digital components.

175. On information and belief, the Cisco '640 Products comprise systems and methods that enable a control object capable of specifying a dynamic control logic depending on the intercepted data communication.

176. On information and belief, the Cisco '640 Products enable applying by the intercept application the dynamic control logic specified by the control object on the digital object.

177. On information and belief, the Cisco '640 Products contain functionality for intercepting data communication between a first application and a second application within a computer network without changing the functionality of the first application and the second application.

178. On information and belief, Cisco has directly infringed and continues to directly infringe the '640 patent by, among other things, making, using, offering for sale, and/or selling digital rights technology, including but not limited to the Cisco '640 Products, which include infringing technology for controlling the usage of data objects. Such products and/or services include, by way of example and without limitation, the Cisco Cloud Object Storage Release versions 2.2.1, 2.1.2, 3.0.1, 3.5.1, and 3.5.2.

179. By making, using, testing, offering for sale, and/or selling digital rights management products and services, including but not limited to the Cisco '640 Products, Cisco has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '640 patent, including at least claims 1 and 12, pursuant to 35 U.S.C. § 271(a).

180. On information and belief, Cisco also indirectly infringes the '640 patent by actively inducing infringement under 35 USC § 271(b).

181. On information and belief, Cisco had knowledge of the '640 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Cisco knew of the '640 patent and knew of its infringement, including by way of this lawsuit.

182. On information and belief, Cisco intended to induce patent infringement by third-party customers and users of the Cisco '640 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Cisco specifically intended and was aware that the normal and customary use of the accused products would infringe the '640 patent. Cisco performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '640 patent and with the knowledge that the induced acts would constitute infringement. For example, Cisco provides the Cisco '640 Products that have the capability of operating in a manner that infringe one or more of the claims of the '640 patent, including at least claims 1 and 12, and Cisco further provides documentation and training materials that cause customers and end users of the Cisco '640 Products to utilize the products in a manner that directly infringe one or more claims of the '640 patent. By providing instruction and training to customers and end-users on how to use the Cisco '640 Products in a manner that directly infringes one or more claims of the '640 patent, including at least claims 1 and 12, Cisco specifically intended to induce infringement of the '640 patent. On information and belief, Cisco engaged in such inducement to promote the sales of the Cisco '640 Products, e.g., through Cisco user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '640 patent. Accordingly, Cisco has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '640 patent, knowing that such use constitutes infringement of the '640 patent.

183. The '640 patent is well-known within the industry as demonstrated by the over 47 citations to the '640 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Google, Inc. and International Business

Machines Corporation). Several of Cisco's competitors have paid considerable licensing fees for their use of the technology claimed by the '640 patent. In an effort to gain an advantage over Cisco's competitors by utilizing the same licensed technology without paying reasonable royalties, Cisco infringed the '640 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

184. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '640 patent.

185. As a result of Cisco's infringement of the '640 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Cisco's infringement, but in no event less than a reasonable royalty for the use made of the invention by Cisco together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff MOV Intelligence respectfully requests that this Court enter:

- A. A judgment in favor of Plaintiff MOV Intelligence that Cisco has infringed, either literally and/or under the doctrine of equivalents, the '230 patent, the '006 patent, the '516 patent, the '504 patent, the '418 patent, the '114 patent and the '640 patent;
- B. An award of damages resulting from Cisco's acts of infringement in accordance with 35 U.S.C. § 284;
- C. A judgment and order finding that Defendant's infringement was willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate within the meaning of 35 U.S.C. § 284 and awarding to Plaintiff enhanced damages.
- D. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees against Defendant.
- E. Any and all other relief to which MOV Intelligence may show itself to be entitled.

JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, MOV Intelligence requests a trial by jury of any issues so triable by right.

Dated: September 23, 2016

Respectfully submitted,

/s/ Dorian S. Berger
Elizabeth L. DeRieux (TX Bar No. 05770585)
D. Jeffrey Rambin (TX Bar No. 00791478)
CAPSHAW DERIEUX, LLP
114 E. Commerce Ave.
Gladewater, Texas 75647
Telephone: 903-236-9800
Facsimile: 903-236-8787
E-mail: ederieux@capshawlaw.com
E-mail: jrambin@capshawlaw.com

OF COUNSEL:

Dorian S. Berger (CA SB No. 264424)
Daniel P. Hipskind (CA SB No. 266763)
BERGER & HIPSKIND LLP
1880 Century Park East, Ste. 815
Los Angeles, CA 95047
Telephone: 323-886-3430
Facsimile: 323-978-5508
E-mail: dsb@bergerhipskind.com
E-mail: dph@bergerhipskind.com

*Attorneys for Marking Object Virtualization
Intelligence, LLC*