Additionally, the term "private call" in "private call key variable" is synonymous with a secure communication, *i.e.*, a point-to-point communication. *See* JX-3 at col. 6, lns. 51-65 ("The present invention provides method for point-to-point communications (secured private calls) within secure communications systems"). As the '571 patent specification explains, "[a] private call key variable is generated . . . by modifying an encryption key variable of the limited set of encryption key variables based on a predetermined function." JX-3 at col. 2, lns. 35-38. By creating this private call key variable, communication units "are free to engage in a secure point-to-point communication without other communication units in the secure system being able to eavesdrop . . . ." *Id.* at col. 2, lns. 45-49 (emphasis added).

B. Infringement Analysis of the '571 Patent

Microsoft argues that Motorola has failed to show that anyone has ever performed the method steps of all asserted claims of the '571 patent. Resp. Br. at 10. According to Microsoft, it is not enough to show that a particular article is capable of performing the claimed steps; instead, the patentee must show that each step is actually performed in the United States. *Id.* (citing *Joy Techs., Inc. v. Flakt, Inc.*, 6 F.3d 770, 775 (Fed. Cir. 1993)). Microsoft's argument is rejected.

Motorola's infringement claims are based, in part, on the Xbox's implementation of the IEEE's 802.11 standard, colloquially known as Wi-Fi, and the normal use of the Xbox with Wi-Fi in a home environment. As confirmed by Microsoft's own admissions, the Xbox products are compliant with the IEEE 802.11 standard. *See, e.g.*, CX-708C (Acampora WS) at 87-95; CX-22; CX-23; CX-378C; CX-379C; CX-643C (Casebolt Tr. 38-39, 57, 79, 81, 88, 96-98); CX-648C (McClive Tr. 95-96, 132); CX-653C (Steiner Tr.

12, 35-41, 54, 97-100); CX-654C (Caruana Dep. Tr.) at 9-21, 30, 36-37, 116-117, 154. For all purposes pertinent to this investigation, the IEEE 802.11 standard is fully and completely described in a standards document referred to as "802.11-2007." CX-708C (Acampora WS) at 86-87; CX-383. The 802.11-2007 document therefore also describes a product that complies with the standard, including the Xbox. CX-708C (Acampora WS) at 86-87.

1. Accused Products

Motorola argues that the accused products are Microsoft's Xbox 360 console, including the Xbox 360 S 4 GB and 250 GB consoles, as well as the Xbox 360 Wireless N Adapter (collectively, "the Xbox"), imported into the United States, and/or sold after importation. Compls. Br. at 169-70 (citing CX-708C (Acampora WS) at 86 and Tab D).

Microsoft argues that Motorola failed to provide any evidence that the accused products that contain [ ] infringe the '571 patent. Resp. Br. at 8-10. Microsoft asserts that "[a]ll Wireless N Adapter products currently being sold use the [ ] and certain Xbox consoles contain a [ ] that uses the [ ]" *Id.* at 8 (citing RX-317C (Caruana WS) at Q29). Microsoft explains that "Motorola was aware of these [ ] and took discovery on these devices." *Id.* (citing CX-654C (Caruana Dep. Tr.) at 33-36). It is argued that "Motorola nevertheless chose not to perform an infringement analysis on any of these Atheros-based devices." *Id.* (citing CX-708C (Acampora WS) at Tab E, p. 2 ("Other Xbox products use, or are planned to use, WiFi chips from [ ]. This analysis focuses on the [ ] WiFi chip").

Motorola argues that "Microsoft apparently seeks to exploit discovery misconduct and to end-run the Commission's enforcement remedies." Compls. Reply Br. at 51. Motorola contends that "there is no basis for entering specific findings with respect to [ ] Xbox products." *Id.* at 52. Motorola asserts that "[t]o date, no Xbox product with an [ ] has been imported," and that "Microsoft has not contended otherwise." *Id.*

Motorola explains:

> Early in this Investigation, Motorola interrogatories required Microsoft to identify all Xbox products that were "currently being, ***or in the next twelve (12) months will be*** … imported." CX-629C at 9. Those interrogatories further requested identification of the chip contained in such product. *Id.* at 9-10. In response, Microsoft identified only the Xbox product code-named [ ] Microsoft's name for Xbox products using [ ] chips. CX-630C at 17. And Microsoft only identified [ ] chips. CX-630C at 18 ("The Xbox 360 S 250 GB and Xbox 360 S 4 GB Consoles use the [ ] Wi-Fi chip."), 22 ("The Xbox 360 S 250 GB and Xbox 360 S 4GB consoles use a wireless module assembly provided by [ ]"). Microsoft supplemented its response on April 22, 2011, but did not identify [ ] or any other chip manufacturer. CX-631C at 4-5. Microsoft did not further supplement.
>
> In addition, two Microsoft corporate deposition witnesses confirmed (as late as June 24, 2011, three weeks before the close of fact discovery) that imported Xboxes did not contain [ ] chips, and that Xboxes with [ ] chips had not yet even left the factory. CX-643 (Casebolt) at 125, 127-28; CX-654C (Caruana [Dep. Tr.]) at 34-35. Long after discovery closed, Microsoft employee Casebolt testified in his September 9, 2011 direct written testimony that the Xbox with [ ] was still not being shipped. RX-314C at 8.

Id. at 52-53.

First, RX-317C (Caruana WS) does not support Microsoft's assertion that "[a]ll Wireless N Adapter products currently being sold use the [ ] and certain Xbox consoles contain a [ ] that uses the [ ]." Q29 states:

"**Which wireless networking products use Atheros chipsets?**" Mr. Caruana's answer is: [ ] RX-317C (Caruana WS) at Q29 (emphasis in original). In reality, the question and answer is silent about whether these [ ] products are "currently being sold."

If in fact Microsoft has imported Xbox products containing [ ] Microsoft has violated its discovery obligations under 19 C.F.R. 210.27(c) by failing to satisfy its "duty seasonably to amend a prior response to an interrogatory … or request for admission." Moreover, the parties have not presented evidence and arguments specifically addressing new products containing [ ].

Accordingly, the administrative law judge is not making any factual findings on whether Xbox products containing [ ] are non-infringing.

2. Direct Infringement

For the reasons set forth below, Motorola has shown that Microsoft's accused products directly infringe all asserted claims of the '571 patent.

Claim 12

The preamble of independent method claim 12 recites:

> **In a secure communication system that includes a plurality of communication units, wherein each communication unit of the plurality of communication units stores a limited set of encryption key variables, a method for a communication unit of the plurality of communication units to receive a point-to-point communication within the secure communication system, the method comprises the steps of:**

Motorola has satisfied the preamble.

The claim term "communication unit" has been construed to mean "a unit that

communicates." The claim term "encryption key variable" has been construed to mean "a dynamic parameter used to reduce unauthorized eavesdropping of transmitted communication in a communication system." The claim term "point-to-point communication" has been construed to mean "secure communication between two or more communication units."

When the Xbox is used with a Wi-Fi router, with both set for WPA or WPA2 security, the Xbox and the router are communication units in a secure communication system, with point-to-point communication between the router and the Xbox. CX-708C (Acampora WS) at 123. The infringing use consists of Wi-Fi communication between the Xbox and the Wi-Fi router. That a router can be a communication unit is confirmed by the fact that the ASTRO system, cited in the '571 specification as an exemplary communication unit, included router units that could encode/decode a wireless communication to allow wireless users to connect to a wired phone network, just as a Wi-Fi router allows a wireless user to connect to the wired Internet. Banwart Tr. 727-728, 731.

The claim term "encryption key variable" has been construed to mean "a dynamic parameter used to reduce unauthorized eavesdropping of transmitted communication in a communication system."

When set for WPA or WPA2 security, the Xbox and the router store a limited number of encryption key variables. In particular, [

] CX-708C (Acampora WS) at 124; Acampora Tr. 932; Caruana Tr. 1157; Geier Tr. 1216. [

] CX-386. [

] Geier Tr. 1216. After that initial login, [ ]. Geier Tr. 1216; CDX-14 and CDX-15 (demonstrating login and reconnection process). Also, as required by the parties' agreed-upon construction of the preamble, [ ] CX-708C (Acampora WS) at 125-135, 153-156; CDX-17; Geier Tr. 1216; CX-654C (Caruana Dep. Tr.) at 75, 161-63; CX-387C. The passphrase of the router is an encryption key variable, a dynamic parameter used to reduce unauthorized eavesdropping of transmitted communication in a communication system. CX-708C (Acampora WS) at 124-129.

Microsoft argues that the stored passphrase is not an encryption key variable. Microsoft argues that under its claim construction, the encryption key variable must be used by an encryption/decryption algorithm to uniquely encrypt/decrypt data. RRX-23C (Geier RWS) at 34-40. Microsoft's proposed claim construction was rejected, *supra*.

Step a) of claim 12 recites:

> **a) receiving, by the communication unit, identity of an encryption key variable and information pertaining to a predetermined function, wherein the identity of the encryption key variable and information pertaining to the predetermined function have been transmitted by a transmitting communication unit;**

Motorola has satisfied this claim step.

The claim term "identity of an encryption key variable" has been construed to mean "an identifier that is capable of uniquely identifying which encryption key variable of the limited set is being used."

Xbox consoles when used with an 802.11-compliant router, with both set for

WPA or WPA2 security, infringe this step. The Xbox is the receiving communication unit, and the router is the transmitting communication unit. When the Xbox is turned on after having been previously connected (discussed above), it issues a "Probe Request," to which the router responds with a "Probe Response." CX-708C (Acampora WS) at 145-46. The Probe Response includes a value called the "Service Set Identifier" (SSID), which is the name of the network that the router is connected to. *Id.* at 146; CX-383 at Section 7.2.3.9. The SSID identifies the previously stored passphrase (*i.e.*, the encryption key variable). CX-708C (Acampora WS) at 153-156; CX-387C. Thus, the SSID is the "identity of an encryption key variable." CX-708C (Acampora WS) at 146-147.

The Probe Response also includes a value called the "Basic Service Set Identification" (BSSID). *Id.* at 147-149, 152-153, 157. The BSSID is the network address of the router, which uniquely identifies the router. *Id.* at 147. After the Xbox has received the probe response from the router, the router and the Xbox exchange a series of messages called the "4-Way Handshake." CX-708C (Acampora WS) at 106-108, 147. During this process, a value called the "ANonce" is sent from the router to the Xbox.[78] *Id.* at 147, 151-153, 158; CDX-13; CX-365C; Geier Tr. 1198-99. The ANonce is a unique random number generated by the router during the 4-Way Handshake. CX-708C (Acampora WS) at 150-51. The BSSID and ANonce values are the "information pertaining to the predetermined function" because, as discussed below in connection with step b), they are used in a predetermined function to generate the private call key variable (see below). CX-708C (Acampora WS) at 148.

[78] "Nonce" stands for "number used once," and the "A" indicates that it is generated by the "Authenticator," which in this instance is the router. *See* CX-383 at 11, 17.

Microsoft is incorrect when it argues that the "identity" of the encryption key variable must be unique to the entire universe of communication systems practicing the patented invention. Basically, Microsoft is arguing that if the invention is implemented in one system (*e.g.*, Washington) by using the numbers 1, 2, 3, etc., to identify the stored encryption keys, there could only be one such system in the world, because the moment a second system is created elsewhere (*e.g.*, Baltimore) that also uses 1, 2, 3, etc., the identifiers are no longer unique, even though they are unique within each system. Such a construction excludes the preferred embodiment (police systems in multiple municipalities) from coverage — an unsound approach. The SSID is undeniably an identifier that is capable of uniquely identifying which encryption key variable of the limited set is being used.

Step b) of claim 12 recites:

> **b) generating, by the communication unit, a private call key variable based on the encryption key variable and the information pertaining to the predetermined function; and**

Motorola has satisfied this claim step.

The claim term "private call key variable" has been construed to mean "a dynamic parameter used in a point-to-point communication in a communication system."

The Xbox operating in conjunction with an 802.11-compliant router, with both set for WPA or WPA2 security, infringes this claim step. During the 4-Way Handshake, described above, the Xbox generates an encryption key called the "Pairwise Transient Key" (PTK), which is the private call key variable of the claim. CX-708C (Acampora WS) at 158; Geier Tr. 1196, 1204-1205. The passphrase, which is the encryption key

variable, and the BSSID and the ANonce, which make up the information pertaining to the predetermined function, are used to generate the PTK.

In particular, the passphrase is used in a "hash function" to generate the PSK. CX-708C (Acampora WS) at 136, 159. Caruana Tr. 1158; Geier Tr. 1216 (the PSK is generated from the passphrase each time the Xbox is turned on). For home wireless networks, including those used with the Xbox, the PSK is used as the "Pairwise Master Key" (PMK), which is another encryption key used in the 802.11 standard. CX-708C (Acampora WS) at 159; Acampora Tr. 933-934; Geier Tr. 1196. The PMK in turn is used with other values to generate the PTK. Thus, the PTK is generated based on the passphrase, *i.e.*, the "encryption key variable." CX-708C (Acampora WS) at 159; Acampora Tr. 934; Geier Tr. 1197-1198.

Additionally, the PTK is generated based on the ANonce and the BSSID, which are "information pertaining to the predetermined function." *Id.* at 159-162; Geier Tr.1198-1200; CX-383 at Section 8.5.1.2; CX-404C at 10.

The PTK is the dynamic parameter generated by the 4-Way Handshake each time the connection process between the Xbox and router takes place (after an Xbox is powered on). Thus, the PTK is the private call key variable of asserted claim 12.

Step c) of claim 12 recites:

> **c) utilizing the private call key variable to privately communicate with the transmitting communication unit.**

Motorola has satisfied this claim step.

The Xbox operating in conjunction with an 802.11-compliant router, with both set for WPA or WPA2 security, infringes this claim step. The Xbox uses the private call key

variable (the PTK) to privately communicate with the router. CX-708C (Acampora WS) at 162. In particular, per the 802.11 standard, a portion of the PTK called the "temporal key" (TK) is used to encrypt the data that is communicated. CX-708C (Acampora WS) at 162-168; Acampora Tr. 934-935; CX-383 at Section 8.5.1.2, Fig. 8-4 (applicable to WPA encryption), Fig. 8-16 (applicable to WPA2 encryption); CX-365C; CX-654C (Caruana Dep. Tr.) at 70-71; CX-415C; CX-393C at MRVL000687-691; CX-404C at 10-12.

Claim 13

Dependent claim 13 recites:

> **In the method of claim 12, step (b) further comprises generating the, private call key variable by modifying the encryption key variable based on information pertaining to the predetermined function, wherein the information pertaining to the predetermined function includes, at least in part, a unique identification code of the communication unit, a unique identification code of the transmitting communication unit, or a combination of the unique identification code of the communication unit and the unique identification code of the transmitting communication unit.**

Motorola has satisfied this claim.

As discussed above, the Xbox generates the private call key variable (the PTK) by modifying the encryption key variable (the passphrase or, equivalently, the PSK) based on, among other things, the BSSID, which is the unique identification code of the router (the transmitting communication unit). CX-708C (Acampora WS) at 168-169; Geier Tr. 1199; CX-383 at Section 8.5.1.2; CX-404C at 10.

3. Indirect Infringement

Motorola has not shown that Microsoft's accused products indirectly infringe all asserted claims of the '571 patent.

Motorola argues that Microsoft induces infringement and contributes to the infringement of independent claim 12 and dependent claim 13 of the '571 patent, as a result of the direct infringement by users of the Xbox (including Microsoft when it tests the Xbox devices) in its typical arrangement in which the user associates the Xbox with a Wi-Fi router configured to use WPA or WPA2 encryption. Compls. Br. at 180-83.

Microsoft argues that Motorola has not established certain required elements of induced infringement and contributory infringement. Resp. Br. at 10-11.

Motorola has made no argument that Microsoft had knowledge that the claimed methods were "both patented and infringing." *Global-Tech*, 131 S.Ct. at 2062. Further, Motorola has not shown that Microsoft possessed specific intent to encourage another's infringement. *Warner-Lambert*, 316 F.3d at 1364. Though Motorola suggests that the operations on which its expert bases his infringement opinion represent "typical" use of the Xbox, Motorola has not offered any proof that these use-case scenarios are actually "typical" or have ever occurred. Indeed, the accused products have many uses that never involve these operations. For instance, the Xbox can be used with no Internet connection (Acampora Tr. 759-760), or with a wired Internet connection, which is non-infringing. *Id.* 745. Further, even when using WiFi, the Xbox can be used without encryption or with WEP encryption—none of which Motorola accuses of infringement. *Id.* 747.

C. Validity of the '571 Patent

For the reasons set forth below, Microsoft has not shown by clear and convincing

evidence that the asserted claims of the '571 patent are invalid.

1. U.S. Patent No. 5,268,962 ("Abadi") (RX-152)

The Abadi patent does not anticipate claims 12 or 13 of the '571 patent. In addition, Microsoft's argument that Abadi in combination with the Takaragi reference renders claim 13 obvious is without merit. CX-720C (Acampora RWS) at 3-16 and Tab A. Abadi solves a problem very different from the problem addressed by the '571 invention: in a system made up of a network of host computers, each host computer having a number of users, there is a need to separate and isolate communications directed to different users in the system, so that one user cannot access communications intended for another. *Id.* at 3; RX-152 at col. 1, ln. 61 to col. 2, ln. 14, col. 2, lns. 39-53. This informs the approach disclosed in Abadi and results in a disclosure significantly different from the '571 patent. CX-720C (Acampora RWS) at 3-4. Abadi discloses two embodiments, neither of which anticipates the asserted claims of the '571 patent. *Id.* at 4.

First, the preamble of claim 12 of the '571 patent, which the parties agree is a limitation of the claim, requires that "each communication unit of the plurality of communication units stores a limited set of encryption key variables." The parties also agree that this phrase in the preamble requires that the encryption key variables must be stored in non-volatile memory. RX-394 at 19. For both Abadi embodiments, the only encryption keys that Microsoft alleges to be encryption key variables are the "Host-to-Host keys." RX-310 (Geier WS) at 17-18; Geier Tr. 1256-1257. However, those Host-to-Host keys are regenerated each time a host computer is powered on or rebooted, and are not stored in non-volatile memory. CX-720C (Acampora RWS) at 4-5; Geier Tr.

1253-1256; RX-152 at col. 3, ln. 55 to col. 7, ln. 52, col. 8, lns. 11-51 and FIGS. 2, 3, 4, 5A and 5B. Therefore, the preamble of claim 12 does not read on Abadi.

Step (a) of claim 12 also requires that the "identity of an encryption key variable" be sent from one communication unit to another. In the first Abadi embodiment, no such identity is sent. Instead, an encrypted version of the Host-to-Host key itself is sent, then decrypted and temporarily stored in volatile memory. CX-720C (Acampora RWS) at 7; Geier Tr. 1252. Microsoft's proposed claim construction requirement that sending the key itself is the same thing as sending the identity of the key has been rejected. As discussed, *supra*, the '571 patent requires that the encryption key variables are already permanently stored in each communication unit, and the identity that is received by a communication unit is then used to select the previously stored key. Geier Tr. 1247, 1248, 1250. Abadi's first embodiment is completely different: the transmitting host computer sends the key to the receiving host computer, which decrypts the received key to extract a host-to-host key, instead of using the received key to identify a key that is already stored in that unit. RX-152 at col. 6, lns. 29-31; Geier Tr. 1252.

Regarding claim 13, Microsoft argues that a value called the "Buffer Queue Index" (BQI) is the unique identification code of the communication unit. RX-310 (Geier WS) at 22; Geier Tr. 1263. Unlike the unique identification code, which identifies a communication unit, the BQI instead identifies one of the users at the destination host computer, and does not identify the destination host computer itself. Geier Tr. 1257; CX-720C (Acampora RWS) at 13. That is, Abadi teaches that there are multiple users, and therefore multiple BQIs, for a single host computer, so none of the BQIs uniquely identifies the host computer. CX-720C (Acampora RWS) at 13, Acampora Tr. 2314.

Microsoft argues in the alternative it would have been obvious to combine Abadi with the Takaragi reference, discussed *infra*, to supply the unique identification of the communication unit. RX-310 (Geier WS) at 22-23. In the first place, the systems of Abadi and Takaragi are very different. Abadi discloses a switched network of host computers that communicate with one another on a point-to-point basis. Geier Tr. 1266. Each packet of data sent over the network has a destination address in the header of the packet, and switches in the network route the packet so that only the destination host computer, and no other host, receives the packet. RX-152, Fig. 2; Geier Tr. 1265-66. In contrast, as discussed *infra*, the system of Takaragi is a broadcast system, in which any one of a number of terminals broadcasts messages to every other terminal in the system. The other terminals each receive the message, and examine a destination indicator in the message to determine whether or not to decode the message. Geier Tr. 1274. Thus, one of ordinary skill would have little suggestion or motivation to use the destination identification methods of one system in the other, entirely different system. Geier Tr. 1274-1275.

In addition, Microsoft alleges that the "office number" of Takaragi would be the required unique identification of the communication unit. RX-310 (Geier WS) at 22-23. But the office number of Takaragi identifies an office, not a communication unit. CX-720C (Acampora RWS) at 28. In addition, Abadi already uses the destination address of the destination host computer in the header of the packets that it sends during communication. RX-152, FIG. 2, col. 9, lns. 3-4; Geier Tr. 1263-1265. Abadi does not use this unique identification of the communication unit in its algorithm for generating the encryption key used for communication. *Id.* Microsoft fails to explain why one of

ordinary skill in the art would think to import an office number from the completely different Takaragi system as a substitute for the already-in-place destination address of Abadi.

2. U.S. Patent No. 4,549,308 ("LoPinto") (RX-131)

Microsoft argues that claim 12 is anticipated by the LoPinto patent, and that claim 13 is obvious in light of LoPinto in combination with Abadi or Takaragi. However, neither LoPinto alone, nor in combination with other references, invalidates the '571 patent. CX-720C (Acampora RWS) at 16-23 and Tab B. LoPinto concerns the security of an encryption key used for communications between a cellular radio telephone unit and base stations. LoPinto discloses dynamically changing the encryption key when the cell phone is handed off from one base station to another by mathematically combining a non-broadcast code (NBC) associated with the telephone number with frequency channel values used for the communication. RX-131 at Abstract. The resulting key is then used to encrypt voice communications. CX-720C (Acampora RWS) at 16; RX-131 at col. 1, lns. 56-61.

The plain language of claim 12 of the '571 patent focus on a communication unit, and require that certain actions be performed by that communication unit. LoPinto fails to anticipate claim 12 because neither the mobile phone, nor the base station, nor any other device disclosed in LoPinto, performs all of the actions required by claim 12. CX-720C (Acampora RWS) at 17; Geier Tr. 1267-1268 ("there is no identity [of an encryption key variable] sent from the base station to the telephone"); 1269-1270; Acampora Tr. 2258.

Considering first the preamble of claim 12, the only point-to-point communication involving a plurality of communication units that Microsoft points to in LoPinto is the communication that takes place between a mobile phone and a base station. RX-310 (Geier WS) at 38. And Microsoft's only candidate for an encryption key variable is the NBC. *Id.* at 37; Acampora Tr. 2255. However, even if it is assumed that the mobile phone stores the NBC in non-volatile memory, the base station does not store that value in non-volatile memory, and indeed it would be impractical in a cellular phone system to attempt to store at each base station all the NBCs for all cell phones that happen to pass through that base station's area. Rather, when a particular cell phone connects to a base station, the base station obtains the NBC from a central "mobile telephone switching office." RX-131 at col. 3, lns. 36-41; RX-310 (Geier WS) at 37; Geier Tr. 1271; CX-720C (Acampora RWS) at 20-21. Because the plurality of communication units identified by Microsoft do not all store encryption key variables, the preamble does not read on LoPinto.

Nor does LoPinto disclose a communication unit that satisfies step (a) of claim 12. That element requires a communication unit to receive, from a transmitting unit, two separate things: the "identity of an encryption key variable," and "information pertaining to a predetermined function." No communication unit in LoPinto receives both. CX-720C (Acampora RWS) at 19-20. Microsoft proposes that the telephone number of the cellular telephone can be the "identity of the encryption key variable," but this is incorrect because the cellular telephone does not use any value received from the base station — whether a telephone number or some other value — to identify the phone's own NBC. RX-131 at col. 3, lns. 24-49; CX-720C (Acampora RWS) at 17-18.

Assuming the frequency channel values could be considered "information pertaining...," the telephone does not send those values to the base station. Microsoft also alleges that certain "change key criteria" that are communicated in the system could be the "information pertaining," but the only example of such change key criteria taught in LoPinto are the frequency values, which as already noted are only sent from the base station to the cellular telephone. CX-720C (Acampora RWS) at 19-20. Thus, neither the cellular telephone nor the base station receives the two required values and thus neither fills the role of the receiving communication unit of claim 12, step (a). *Id.*; Geier Tr. 1267-70.

As to claim 13, LoPinto does not use a unique identification code of a communication unit to generate the private call key variable. Microsoft relies upon combinations of LoPinto with Abadi or Takaragi to fill this gap. RX-310 (Geier WS) at 40-42. This approach is mistaken because the system of LoPinto has no need for the BQI of Abadi or the office number of Takaragi (the values that Microsoft alleges are communication unit identifiers). Moreover, even if a person of ordinary skill were to combine LoPinto with Abadi or Takaragi, the elements cited by Microsoft are not unique identification codes. As described, *supra*, the BQI does not identify a communication unit but instead describes a user. CX-720C (Acampora RWS) at 13; Acampora Tr. 2313-14. Likewise, the "office number" of Takaragi does not uniquely identify a particular communication unit, as explained next. CX-720C (Acampora RWS) at 28.

3. U.S. Patent No. 5,309,516 ("Takaragi") (RX-173)

Microsoft argues that Takaragi anticipates claims 12 and 13 of the '571 patent, and in the alternative Microsoft asserts that claim 13 is rendered obvious by Takaragi in

combination with Abadi. Neither argument has merit. CX-720C (Acampora RWS) at 23-31 and Tab C.

As a threshold matter, Takaragi is not prior art to the '571 patent because the preparation of the application that issued as the '571 patent, filed July 1, 1993 (and mailed to the Patent Office on June 29, 1993), was ongoing before the June 15, 1993 filing date of the Takaragi patent. The testimony of Dean Banwart (inventor) and Timothy Markison (patent attorney), as corroborated by contemporary records (JX-4 at MOTM_ITC0000144; CX-677C; CX-679C), establishes that the invention was conceived, and a near-final draft of the application prepared, prior to June 15, and that between June 15 and June 29 the application was being finally reviewed by the inventor. CX-709C (Banwart) 5-8; Banwart Tr. 718-19; CX-710C (Markison) 3-7; Markison Tr. 2465-68; CX-677C; CX-679C. Prior conception, accompanied by diligence towards constructive reduction to practice from before the effective date of the prior art reference until the filing date of the patent in suit, takes the reference out of the prior art. *Mahurkar v. C.R. Bard, Inc.*, 79 F.3d 1572, 1576-79 (Fed. Cir. 1996) (finding publication not to be prior art because patentee had shown earlier conception and reasonable diligence in reducing to practice).

Takaragi is thus not prior art because the '571 invention was conceived (and the application in a near-final state) prior to the Takaragi filing date, and the final review of the application during the June 15-29 period shows diligence towards the July 1 filing date.[79] These facts are sufficiently corroborated by contemporaneous documents and the

[79] Even if Mr. Markison had been preparing the application on June 15-17, the last three days during which he could have possibly worked on the application according to his

testimony of Mr. Banwart and Mr. Markison. *Lacks Indus., Inc. v. McKechnie Vehicle Components USA, Inc.*, 322 F.3d 1335, 1349 (Fed. Cir. 2003) (corroborating evidence of conception "is generally measured under a 'rule of reason' standard" which requires that "an evaluation of all pertinent evidence be made so that a sound determination of the credibility of the evidence may be reached"). Because Motorola has offered evidence to show that Mr. Banwart invented the subject matter of the '571 patent before Takaragi was filed, Motorola has met its burden of production. *Mahurkar*, 79 F.3d at 1577. Microsoft therefore bears the burden of persuasion by clear and convincing evidence that Mr. Banwart did not conceive and thereafter proceed with reasonable diligence as required from before June 15 to the filing date of the '571 patent. *Id.* at 1578. Microsoft has not met this burden.

In any event, Takaragi does not invalidate the '571 patent. Takaragi discloses IC cards (integrated circuit cards) that are inserted into terminal slots and used to encrypt communications between the terminals. CX-720C (Acampora RWS) at 24; Geier Tr. 1277-1278; Acampora Tr. 2263. Each IC card identifies a particular person and a particular office. *Id.* Thus, at different times, a given terminal can be associated with different persons in different offices. *Id.*; RX-173 at Abstract, FIG. 10. A set of master keys is stored in each IC card. CX-720C (Acampora RWS) at 24; Acampora Tr. 2263. Each master key is associated with a particular office or other group of destination terminals. RX-173, col. 5, lns. 40-55. Communications between terminals in the same

---

timesheet, this work would be further evidence of due diligence towards reduction to practice. CX-677C.

office or group use the appropriate master key to encrypt data. CX-720C (Acampora RWS) at 24.

Takaragi does not disclose the requirement in the preamble of claim 12, that the communication units store the encryption key variables. Microsoft cites the master keys used in Takaragi as the encryption key variables, but the master keys are stored on an IC card, which is removable from a communication unit. CX-720C (Acampora RWS) at 27; Acampora Tr. 2263; Geier Tr. 1278.

Also, Takaragi does not disclose the requirement of step (a) of claim 12, that the "identity of an encryption key variable" be received by a communication unit.[80] CX-720C (Acampora RWS) at 225. To initiate an encrypted transmission, a list of all intended receiving persons is generated at the transmitting terminal. RX-173 at col. 7, lns. 11-14. From this, a "destination indicator" is included in each message, which message is transmitted over the communication network to all terminals. Geier Tr. 1274. Microsoft alleges that the destination indicator is the identity of the encryption key variable. RX-310 (Geier WS) at 55. However, the destination indicator does not uniquely identify any master key stored in the IC cards. Rather, the destination indicator is used by an algorithm, depicted in Figure 6 of Takaragi, that selects an appropriate master key. CX-720C (Acampora RWS) at 26-27. Multiple different destination indicators can result in the selection of the same master key.

Microsoft alternatively argues that a value that Takaragi calls the "key information" is the identity of the encryption key variable. RX-310 (Geier WS) at 55.

[80] In addition, Microsoft fails to identify what in Takaragi comprises the alleged "information pertaining to the predetermined function" that is received as required by step (a) of claim 12 of the '571 patent.

However, as Microsoft's expert admitted, there is nothing in the Takaragi disclosure that supports that position. Geier Tr. 1276-77. The only use of the "key information" disclosed in Takaragi is as undefined "information" used to calculate a group key. RX-173 at col. 2, lns. 26-35.

As to dependent claim 13, the destination indicator of Takaragi is not a unique identification code of a communication unit. Microsoft has at different times identified the office number and/or the person identification number as the unique identification of the communication unit. RX-310 (Geier WS) at 51-52, 57. However, neither value identifies a communication unit. The "office" of Takaragi does not refer to a room, but to a geographical location in a large distributed system. This is confirmed by the fact that one of the offices described in Takaragi is the "head office." RX-173 at col. 5, lns. 24-57, col. 6, lns. 21-41 and FIG. 10; CX-720C (Acampora RWS) at 28-29. Also, the person identification number identifies a person, not a communication unit. CX-720C (Acampora RWS) at 29; Acampora Tr. 2262. The person identified by this combination of numbers can go to any communication unit to receive or send a message with the same group key. Geier Tr.1278. If the combination of the office number and person identification number were truly unique to each communication unit, a user moving between two different communication units would use different group keys. CX-720C (Acampora RWS) at 29.

Microsoft, argues in the alternative that it would have been obvious to combine Takaragi with Abadi to cure this deficiency. In the first place, it is significant that Takaragi discloses a broadcast system, in which every message is sent to every terminal in the system. Geier Tr. 1274-75. Each terminal receives the message, and compares the

information on the IC card currently inserted into that terminal to the destination indicator information in the message. If there is a match, the message is accepted. *Id.* 1274. As discussed in connection with Abadi, *supra*, the point-to-point system of that reference is very different from this broadcast system of Takaragi, and so one of ordinary skill would have no incentive to combine the two references. *Id.* 1266.

And even if a person of ordinary skill were somehow to combine Takaragi with Abadi, the combination still does not cure the other deficiencies of Takaragi regarding other missing claim steps of the '571 patent, such as storing a limited set of encryption key variables, or receiving an identity of an encryption key variable and information pertaining to the predetermined function. In addition, the Buffer Queue Index of Abadi serves a function very different from the unique identification code of a communication unit in the '571 patent. As described above, the Buffer Queue Index does not identify a communication unit but instead describes a user. CX-720C (Acampora RWS) at 13, 29.

4. U.S. Patent No. 5,179,591 ("Hardy") (RX-143)

Microsoft argues that claim 12 is anticipated by the Hardy patent, and that claim 13 is obvious in light of Hardy in combination with Abadi or Takaragi. However, neither Hardy alone, nor in combination with other references, invalidates the '571 patent. CX-720C (Acampora RWS) at 31-37 and Tab D. Hardy concerns a method for secure communication between various types of user equipment employing differing cryptography and/or cipher keys. A manual mode and a public key management mode are disclosed. RX-143 at col. 4, lns. 36-39.

In manual mode, Hardy discloses selecting from preset traffic keys that are "physically transported" and manually installed on each terminal. RX-143 at col. 4, lns.

39-43, col. 7, lns. 32-37; CX-720C (Acampora RWS) at 32-33. This is merely a primitive variation on the stored encryption key approach of the prior art that the '571 patent describes in its background section. Microsoft attempts to portray these stored keys as the encryption key variables of claim 12, but Microsoft does not point to anything in the Hardy disclosure that supports this assertion. RX-310 (Geier WS) at 63. The stored keys are not subjected to the steps of claim 12, and are not used to generate new private call key variables. Geier Tr. 1278-79. Rather the keys are simply used for encryption, just like the prior art systems that the '571 patent improved upon. CX-720C (Acampora RWS) at 33. Microsoft's reliance on the manual embodiment of Hardy goes is erroneous, and Microsoft fails to show any possible way that the claims read on the manual mode of Hardy.

As for the public key mode of Hardy, it also falls short. That mode involves the generation of "traffic keys," used for ciphering, through a message exchange. RX-143 at col. 2, lns. 5-8, col. 2, lns. 50-60; CX-720C (Acampora RWS) at 31-32. The terminals involved in the communication generate and exchange two encrypted random numbers, which are then decoded and combined to create the traffic key used for encryption of the communication. RX-143 at col. 6, lns. 20-58; CX-720C (Acampora RWS) at 31-32.

Considering first the preamble of claim 12, the public key mode of Hardy does not disclose storing a limited set of encryption key variables. CX-720C (Acampora RWS) at 33. The random numbers used to calculate the traffic key are generated on the fly and are not stored in non-volatile storage. RX-143 at col. 6, lns. 20-33; CX-720C (Acampora RWS) at 34; Geier Tr. 1279-80. And they are not stored anywhere in the

receiving communication unit prior to step (a), as required by claim 12. Geier Tr. 1246-48, 1250.

Turning to step (a) of claim 12, no communication unit in Hardy receives an identity of an encryption key variable. CX-720C (Acampora RWS) at 34; Geier Tr. 1279-1280. Microsoft attempts to characterize the transmission of the random numbers during the generation of the traffic key as the transmission of the identity of the encryption key variable. RX-310 (Geier WS) at 71. Microsoft is mistaken, because the random number is not a stored encryption key variable and, even if it were, sending the encryption key variable itself cannot satisfy the requirement of sending *the identity* of the encryption key variable. CX-720C (Acampora RWS) at 34. As discussed, *supra*, the identity of the encryption key variable must be used to identify a previously stored encryption key. The sending of the random number identifies nothing that is previously stored. Geier Tr. 1279-80.

Also lacking in Hardy is the step (a) requirement that the communication unit receive "information pertaining to a predetermined function." Microsoft argues that the "capabilities byte," which is exchanged between the terminals, is the information pertaining to the predetermined function, because it specifies a key generation function. RX-310 (Geier WS) at 71. The key generation function, however, is used not to create the traffic key (which is what Microsoft considers the private call key variable), but is instead used *with* the traffic key to encrypt that data. RX-143 at col. 6, lns. 38-41; Geier Tr. 1280-81; CX-720C (Acampora RWS) at 34-35; Acampora Tr. 2269.

As for dependent claim 13, inasmuch as Hardy does not use the unique identification code of a communication unit to generate the encryption key, Microsoft

argues that it would have been obvious to combine Hardy with Takaragi or Abadi to cure this deficiency. RX-310 (Geier WS) at 72-73; CX-720C (Acampora RWS) at 76. As discussed above, one of ordinary skill would not be motivated to borrow ideas from the approaches of Abadi or Takaragi, and even if that were done, neither the BQI of Abadi nor the office number of Takaragi uniquely identifies a communication unit. CX-720C (Acampora RWS) at 36.

5. U.S. Patent No. 5,146,498 ("Smith") (RX-171)

Microsoft argues that claim 12 is anticipated by the Smith patent, and that claim 13 is obvious in light of Smith in combination with Abadi or Takaragi. CX-720C (Acampora RWS) at 38. Neither Smith alone, nor in combination with other references, invalidates the '571 patent. CX-720C (Acampora RWS) at 37-39 and Tab E. Smith discloses a method for remotely changing an encryption key by sending a key change command from a central controller to a radio. RX-171 at Abstract. The command includes an "Opcode" that specifies operations performed on the present key to cause it to change, and also a data field that contains parameters that may be used by the change operation. For example, the command could indicate that the key is to be "XORed" with a data value sent with the command. RX-171 at FIG. 3.

Although Smith discloses storing an initial key, it does not disclose sending the identity of a stored encryption key for use in generating a new key. Acampora Tr. 2325. Significantly, Smith specifically differentiates its approach from an approach that changes keys by sending the identity of a stored encryption key to the communication device. RX-171 at col. 1, lns. 36-42. Smith explains that the prior art approach is inferior because it takes up "vast amounts of memory." RX-171 at col. 1, lns. 42-45.

Thus, Smith teaches away from the '571 patent. CX-720C (Acampora RWS) at 37-38; 1286-87 (Smith does not provide a solution to the problem sought to be solved by both Banwart and Smith).

For dependent claim 13, Microsoft argues that it would have been obvious to combine Smith with Abadi or Takaragi to disclose a unique identification code. RX-310 (Geier WS) at 87-89; CX-720C (Acampora RWS) at 38. As discussed above, one of ordinary skill would not be motivated to borrow ideas from the approaches of Abadi or Takaragi, and even if that were done, neither the BQI of Abadi nor the office number of Takaragi uniquely identifies a communication unit. CX-720C (Acampora RWS) at 38.

D. Domestic Industry (Technical Prong)

Motorola's domestic industry products are Droid 2 and Droid X smart phones (collectively, "Droid").

For the reasons set forth below, Motorola has satisfied the technical prong of the domestic industry requirement with respect to the '571 patent.

Claim 12

The preamble of independent method claim 12 recites:

> **In a secure communication system that includes a plurality of communication units, wherein each communication unit of the plurality of communication units stores a limited set of encryption key variables, a method for a communication unit of the plurality of communication units to receive a point-to-point communication within the secure communication system, the method comprises the steps of:**

Motorola has satisfied the preamble.

The claim term "communication unit" has been construed to mean "a unit that

communicates." The claim term "encryption key variable" has been construed to mean "a dynamic parameter used to reduce unauthorized eavesdropping of transmitted communication in a communication system." The claim term "point-to-point communication" has been construed to mean "secure communication between two or more communication units."

In accordance with the 802.11 standard, when the Droid is used with a router set for WPA or WPA2 security, the Droid and the router are communication units in a secure communication system, with point-to-point communication between the router and the Droid. CX-708C (Acampora WS) at 211-216. The Droid and router store a limited number of encryption key variables, *i.e.*, the passphrase of the router. *Id.* at 212. Also, the Droid stores the passphrase in non-volatile memory. *Id.* at 212.

As it does in the context of infringement, Microsoft disputes that the router is a communication unit, and argues that the passphrase is not an encryption key variable. Microsoft is incorrect for the same reasons as discussed above with respect to infringement.

Step a) of claim 12 recites:

> **a) receiving, by the communication unit, identity of an encryption key variable and information pertaining to a predetermined function, wherein the identity of the encryption key variable and information pertaining to the predetermined function have been transmitted by a transmitting communication unit;**

Motorola has satisfied this claim step.

The claim term "identity of an encryption key variable" has been construed to mean "an identifier that is capable of uniquely identifying which encryption key variable

of the limited set is being used."

As is the case for infringement, the SSID received by the Droid from the router during a probe response is the identity of the encryption key variable, and the BSSID and ANonce received from the router during the 4-Way Handshake make up the information pertaining to the predetermined function. *Id.* at 216-22; CX-365C; CX-437C at 4-8. Microsoft raises the same argument that it does in the infringement context; *viz.*, that the SSID does not uniquely identify the encryption key variable. This argument is incorrect for the same reasons.

Step b) of claim 12 recites:

> **b) generating, by the communication unit, a private call key variable based on the encryption key variable and the information pertaining to the predetermined function; and**

Motorola has satisfied this claim step.

The claim term "private call key variable" has been construed to mean "a dynamic parameter used in a point-to-point communication in a communication system."

The Droid satisfies this claim element in the same way the Xbox infringes it. The PTK is the private call key variable, which is generated form the passphrase, as well as the BSSID and the ANonce. CX-708C (Acampora WS) at 223-25; CX-437C at 8.

Step c) of claim 12 recites:

> **c) utilizing the private call key variable to privately communicate with the transmitting communication unit.**

Motorola has satisfied this claim step.

As is the case for the Xbox's infringement, the Droid uses the PTK in the same

manner to encrypt and decrypt data that is being communicated over the Wi-Fi connection. CX-708C (Acampora WS) at 225-27; CX-365C; CX-437C at 2-4.

Claim 13

Dependent claim 13 recites:

> **In the method of claim 12, step (b) further comprises generating the, private call key variable by modifying the encryption key variable based on information pertaining to the predetermined function, wherein the information pertaining to the predetermined function includes, at least in part, a unique identification code of the communication unit, a unique identification code of the transmitting communication unit, or a combination of the unique identification code of the communication unit and the unique identification code of the transmitting communication unit.**

Motorola has satisfied this claim.

Like for the Xbox, the BSSID is the unique identification of the router. CX-708C (Acampora WS) at 228; CX-383 at Section 8.5.1.2, pp. 198-99; CX-437C at 8.

IX. U.S. Patent No. 5,319,712

U.S. Patent No. 5,319,712 ("the '712 patent") is titled, "Method and Apparatus for Providing Cryptographic Protection of a Data Stream in a Communication System." JX-1 ('712 patent). The '596 patent issued on June 7, 1994, and the named inventors are Louis D. Finkelstein, James J. Kosmach, and Jeffrey C. Smolinske. *Id.* The '712 patent "relates to communication systems and, more particularly, to cryptographic protection within communication systems." *Id.* at col. 1, lns. 7-9 (Field of the Invention).

Motorola asserts independent apparatus claim 6, dependent apparatus claim 8, and independent method claim 17. The asserted claims read as follows:

6. A transmitting communication unit for providing cryptographic protection of a data stream in a communication system having a physical layer, data link layer, and a network layer, transmitting communication unit comprising a data link layer device having:

(a) assigning means for assigning a packet sequence number to a packet derived from a data stream received from the network layer;

(b) updating means, operatively coupled to the assigning means, for updating a transmit overflow sequence number as a function of the packet sequence number; and

(c) encrypting means, operatively coupled to the assigning means and the updating means, for encrypting, prior to communicating the packet and the packet sequence number on the physical layer, the packet as a function of the packet sequence number and the transmit overflow sequence number.

8. The transmitting communication unit of claim **6** wherein the data link layer device further comprises a buffer means, operatively coupled to the encrypting means, for buffering the encrypted packet and the transmitting communication unit further comprises a physical layer device, operatively coupled to the data link layer device, having transmitting means for transmitting the encrypted packet and the packet sequence number associated with the packet on the physical layer.

17. In a communication system having a physical layer, data link layer, and a network layer, a method for providing cryptographic protection of a data stream, comprising:

(a) assigning a packet sequence number to a packet derived from a data stream received from the network layer;

(b) updating a transmit overflow sequence number as a function of the packet sequence number; and

(c) encrypting, prior to communicating the packet and the packet sequence number on the physical layer, the packet as a function of the packet sequence number and the transmit overflow sequence number.

JX-1 at col. 7, lns. 36-54; col. 7, ln. 62 – col. 8, ln. 2; col. 8, ln. 65 – col. 9, ln. 12.

A. Claim Construction[81]

1. The preambles of asserted claims 6 and 17

Claim Term	Motorola's Proposed Constructions	Microsoft's Proposed Constructions
the preambles of asserted claims 6 and 17	*The preambles of asserted claims 6 and 17 limit the respective claims*	*The preambles of asserted claims 6 and 17 do not limit the respective claims*

Motorola argues that the preambles of asserted claims 6 and 17 limit the respective claims. Compls. Br. at 206-08. Microsoft argues that the preambles of asserted claims 6 and 17 do not limit the respective claims. Resp. Br. at 26-28.

As proposed by Motorola, the preambles of asserted independent claims 6 and 17 limit the respective claims.

Whether a preamble limits a claim is decided on a case-by-case basis. *Catalina Mktg. Int'l v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002). "If the claim preamble, when read in the context of the entire claim, recites limitations of the claim, or, if the claim preamble is 'necessary to give life, meaning, and vitality' to the claim, then the claim preamble should be construed as if in the balance of the claim." *Pitney Bowes, Inc. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1305 (Fed. Cir. 1999); *see also Corning*

[81] A person of ordinary skill in the art in the July/August 1993 timeframe was typically a person having at least a bachelor's degree in electrical or computer engineering or equivalent and at least three years of experience working in data communications. This would include working in the field of network communications, including cryptographic protection of data within a communication system, and including the hardware and/or software necessary to implement the cryptographic protection of the data. Common systems in this field included cellular systems, paging systems, telephone systems, and wired or wireless data networking systems. CX-708C (Acampora WS) at 15-16.

Glass Works v. Sumitomo Elec. U.S.A., Inc., 868 F.2d 1251, 1257 (Fed. Cir. 1989). In addition, "dependence on a particular disputed preamble phrase for antecedent basis may limit claim scope because it indicates a reliance on both the preamble and claim body to define the claimed invention." *Catalina Mktg.*, 289 F.3d at 808.

The preambles of claims 6 and 17 are limiting at least to the extent that they require the claimed communication system to have a physical, data link, and network layer. Housley Tr. 1376 (noting that all elements of claim 6 occur in the data link layer); 1379 (noting that it would be consistent for all steps of claim 17 also to occur in the data link layer). As discussed above, the claims and specification confirm that the inventors regarded the multi-layered OSI model as fundamentally related to their invention, and that an important aspect of their invention was that the elements of the claims are located in the data link layer of the OSI model. CX-711C (Kosmach WS) at 3-4. Indeed, elements (a) and (c) in claims 6 and 17 specifically call out "the network layer" and "the physical layer," with the preamble providing antecedent basis for these terms. *See Pitney Bowes*, 182 F.3d at 1306 ("Because this is the first appearance in the claim body of the term "generated shapes", the term can only be understood in the context of the preamble statement "producing on a photoreceptor an image of generated shapes made up of spots.") By calling out "a communication system having a physical layer, data link layer, and a network layer," the preamble establishes that the claimed system complies with the Open Systems Interconnection standard, and provides antecedent basis for terms appearing in the body of the claims.

In addition, for claim 6, all the elements of the claim are part of "a data link layer device." The phrase, "a data link layer device" is unquestionably part of the required

elements of the claim, given that the phrase follows the word "comprising" in the preamble. JX-1 at col. 7, lns. 36-54. Claim 8, which depends from claim 6, further confirms that the elements of claim 6 must be part of a data link layer device (*i.e.*, must be in the data link layer) — claim 8 requires that "the data link layer device further comprises a buffer means … for buffering the encrypted packet…," and it goes on to require a separate "physical layer device" that receives the encrypted data from the data link layer device and transmits it. JX-1 at col. 7, ln. 62 to col. 8, ln. 2

Claim 17, being a method claim, does not include the claim 6 phrase, "data link layer device." JX-1 at col. 8, ln 65 to col. 9, ln. 12. However, because claim 17 is the method claim counterpart of apparatus claim 6, with identical structure and wording as to substantive content (*see* CDX-310, reproduced below), and upon consideration of the importance that the specification attributes to operation in the data link layer, one of ordinary skill in the art would conclude that the steps of claim 17 must be performed in the data link layer.

The logical structure of both claims 6 and 17 also confirms that the elements of claim 6 and the steps of claim 17 are each in the data link layer. Element (a) in each claim specifies receipt of a data stream from "the network layer," and element (c) requires that the encrypted data packet be communicated on the physical layer. JX-1 at col. 7, lns. 36-54, col. 8, ln. 65 to col. 9, ln. 12.[82] It follows from the hierarchy of the OSI

[82] The phrase "prior to communicating the packet … on the physical layer" in step (c) only makes sense if encryption must occur before data enters the physical layer. (If encryption could occur in the physical layer, then it goes without saying that encryption must occur before communication). A construction that renders claim language superfluous or meaningless is unsound. *Bicon, Inc. v. Straumann Co.*, 441 F.3d 945, 950 (Fed. Cir. 2006).

model that the actual structure and operations of the elements of the claim take place in the data link layer.

2. "assigning means" (claim 6)

Claim Term	Motorola's Proposed Construction	Microsoft's Proposed Construction
"assigning means" (claim 6) *Function*	*Function*: assigning a packet sequence number to a packet derived from a data stream received from the network layer	
"assigning means" (claim 6) *Structure*	*Structure:* a counter and related structure (116) implemented in hardware and/or software	*Structure: This term is indefinite because the corresponding structure is not sufficiently described in the specification.*

The claim term "assigning means" appears in elements (a), (b), and (c) of claim 6. JX-1.

Both parties construe the function of the term to mean "assigning a packet sequence number to a packet derived from a data stream received from the network layer."

Motorola construes the structure of the term to mean "a counter and related structure (116) implemented in hardware and/or software." Compls. Br. at 209. Microsoft argues that this claim term is indefinite because the corresponding structure is not sufficiently described in the specification. Resp. Br. at 23.

As proposed by both parties, the function of the claim term "assigning means" is construed to mean "assigning a packet sequence number to a packet derived from a data stream received from the network layer."

As proposed by Motorola, the structure of the claim term "assigning means" is construed to mean "a counter and related structure (116) implemented in hardware and/or

software."

Microsoft asserts that this claim is indefinite because there is insufficient disclosure of structure, but Microsoft is wrong. RRX-24C (Housley RWS) at 44. The structure disclosed in the specification is a counter and related structure (116) implemented in hardware and/or software. CX-708C (Acampora WS) at 76. Column 5, lines 15-17 disclose that "[a] packet sequence number is assigned 116 to each packet of the plurality of packets." JX-1 ('712 patent). FIG. 1 shows block 116, which assigns a sequence number to each packet. *Id.* The specification discloses that when the packet sequence number "rolls over (*e.g.*, indicated by an overflow signal 122), the 24 bit long overflow counter 124 is incremented." JX-1 at col. 3, lns. 65-68. In addition, Figure 1, as described in the specification at column 5, lines 23-28, discloses that the block 116 provides the overflow signal 122 to block 124, and provides a 7-bit sequence number to block 106. Given this explicit disclosure, it would be apparent to a person skilled in the art that block 116 includes a counter that counts the packets sent to it from block 114. CX-708C (Acampora WS) at 76. A counter is the structure that would generate a count, "roll over," and generate a "roll over" signal. *Id.* Counters are well known in the field of data communication systems, and are implemented in hardware and in software. *Id.* *See Atmel Corp.*, 198 F.3d at 1379-80 (stating that disclosed structure may be implicit in patent's written description if clear to a person of ordinary skill in the art); *Creo Prods., Inc. v. Presstek, Inc.*, 305 F.3d 1337, 1347 (Fed. Cir. 2002). As recently held by the Federal Circuit in *HTC Corp. v. IPCom GmbH & Co., KG*, 2012 WL 254804 at *8 (Fed. Cir. 2012):

> "Whether a specification adequately sets forth structure corresponding to a claimed function is viewed from the perspective of one skilled in the art.... Although the specification here does not literally disclose a processor and transceiver, a person skilled in the art would understand that the mobile device would have to contain a processor and transceiver."

Indeed, Microsoft's own expert agrees that a counter is included in the "assigning means." Housley Tr. 1383.

The implementation of a counter in hardware and/or software is well known to those skilled in the art. CX-708C (Acampora WS) at 78; Housley Tr. 1384. Thus, given the disclosure of a counter, the requirements of Section 112(6) are satisfied. *See Intel Corp. v. VIA Techs., Inc.*, 319 F.3d 1357, 1365-67 (Fed. Cir. 2003) (holding that the internal circuitry of an electronic device need not be disclosed if one of ordinary skill in the art would understand how to build and modify the device); *S3, Inc. v. NVIDIA Corp.*, 259 F.3d 1364, 1370-71 (Fed. Cir. 2001) (noting that "selector" was an adequate corresponding structure for performing the "selectively receiving" function even though neither the electronic structure of the selector nor details of its electronic operation were described in the specification); *In re Dossel*, 115 F.3d 942, 946-47 (Fed. Cir. 1997) (The structure was determined to be a general-purpose computer, even though the word "computer" was not used in the specification).

A person of ordinary skill in the art would also understand that block 116 includes related structure associated with the counter for assigning the sequence number to the packet.[83] CX-708C (Acampora WS) at 77. Specifically, when block 116 receives a

[83] *See* U.S. Patent Number 5,222,061 (CX-374), issued in June 1993, which discloses the well-known use of a counter and associated circuitry, such as that disclosed in block 116,

packet, the counter is advanced in response to receipt of the packet, and the new sequence number is presented at the output structure of the counter. *Id.* At this point, the count is assigned to the packet.[84] *Id.*

As discussed, *infra*, Microsoft also argues that the function of the assigning means includes segmentation. RRX-24C (Housley RWS) at 29. Based on that erroneous construction, Microsoft attempts to impose a requirement that, as part of the Section 112(6) analysis of the "assigning means," a structure for segmenting the data stream must be disclosed. However, as demonstrated, *infra*, the function of the assigning means does not include segmentation, and therefore no segmentation structure need be disclosed insofar as this claim element is concerned. Acampora Tr. 983-984.

3. " packet" (claims 6, 8 and 17)

Claim Term	Motorola's Proposed Construction	Microsoft's Proposed Construction
"packet" (claims 6, 8 and 17)	a unit of data that includes a header that is used for identification and routing purposes, conforming to the OSI protocol model	a discrete unit of data derived from a data stream, which includes a header having a "packet sequence number"

The claim term "packet" appears in elements (a) and (c) of independent apparatus

---

to assign packet sequence numbers to packets. Specifically, "sequence number generator 125" is disclosed as a conventional modulo M counter, which generates packet sequence numbers. The patent explains that "[a]s is well-known, a counter, such as generator 125, advances the value of a current count to a next, succeeding value." *Id.* at col. 3:7-20. This counter is associated with circuitry that "accepts via bus 126 the current value generated by generator 125 and adds the value as a packet sequence number to the latest data packet that controller 120 unloads from transmit buffer." CX-708C (Acampora WS) at 78.

[84] The association of the count to the packet must be maintained as the packet and counter flow through the system, as shown in FIG. 1 of the '712 patent. However, that aspect of system operation is not part of the function of the assigning means, and so is not subject to the Section 112(6) analysis.

claim 6, in dependent claim 8, and in elements (a) and (c) of independent method claim 17. JX-1.[85]

Motorola construes the term to mean "a unit of data that includes a header that is used for identification and routing purposes, conforming to the OSI protocol model." Compls. Br. at 211. Microsoft construes the term to mean "a discrete unit of data derived from a data stream, which includes a header having a 'packet sequence number'." Resp. Br. at 28.

As proposed by Motorola, the claim term "packet" is construed to mean "a unit of data that includes a header that is used for identification and routing purposes, conforming to the OSI protocol model."

The materials submitted with the '712 patent application confirm that a packet is a unit of data that includes a header that is used for identification and routing purposes. JX-2 at MOTM_ITC0000086, 91-92. In the '712 patent, packets conform to the OSI model. JX-1 at col. 2, lns. 55-57, col. 3, lns. 59-65. Reference to the standards document that defines the OSI Model confirms that data is communicated via the OSI model in packets (which the OSI model refers to as "data units") with headers that include identification and routing information (which the OSI model refers to as "control information"). CX-369 at Section 5.6; CX-708C (Acampora WS) at 74.

Microsoft's proposed definition unnecessarily incorporates the limitation "having a 'packet sequence number,'" but this limitation is already imposed by the claim language itself. RRX-24C (Housley RWS) at 26. Additionally, Microsoft's definition fails to acknowledge that the claimed inventions are strictly confined to the OSI model.

[85] The term also appears in non-asserted claims. JX-1.

CX-711C (Kosmach WS) at 4. Microsoft's definition would embrace systems well outside of the OSI model that did not have packet headers used for identification and routing purposes.

4. " packet sequence number" (claims 6, 8 and 17)

Claim Term	Motorola's Proposed Construction	Microsoft's Proposed Construction
"packet sequence number" (claims 6, 8 and 17)	a multi-bit incrementing number that is transmitted along with the "packet"	a multi-bit incrementing number assigned to sequence "packets" during reassembly that is transmitted along with the "packet"

The claim term "packet sequence number" appears in elements (a), (b), and (c) of independent apparatus claim 6, in dependent claim 8, and in elements (a), (b), and (c) of independent method claim 17. JX-1.[86]

Motorola construes the term to mean "a multi-bit incrementing number that is transmitted along with the 'packet'." Compls. Br. at 212. Microsoft construes the term to mean "a multi-bit incrementing number assigned to sequence 'packets' during reassembly that is transmitted along with the 'packet'." Resp. Br. at 24.

As proposed by Motorola, the claim term "packet sequence number" is construed to mean "a multi-bit incrementing number that is transmitted along with the 'packet'."

Motorola's construction is consistent with the patent claims and use of the term in the specification. JX-1 at col. 3, lns. 62-65, col. 5, lns. 29-32 ("The encrypted plurality of packets and the packet sequence number associated with each packet are transmitted on the physical layer...."); CX-708C (Acampora WS) at 74-75.

[86] The term also appears in non-asserted claims. JX-1.

Microsoft's proposed construction, however, improperly limits a "packet sequence number" to a particular *use* ("to sequence 'packets' during *reassembly*") that is not part of the claim. *See Ecolab, Inc. v. Envirochem, Inc.*, 264 F.3d 1358, 1367 (Fed. Cir. 2001) ("Where the function is not recited in the claim itself by the patentee, we do not import such a limitation."). The "packet sequence number" is generated and assigned to a packet, prior to movement of the packet from "layer 2" to "layer 1," for transmission. JX-1 ('712 patent) at Fig. 1 (102). The claims at issue do not address how information is processed *after* transmission when it is *received* from layer 1, much less how data is reassembled or whether the same sequence number used for encryption is used for reassembly.

Significantly, the specification explains that, in one embodiment, the sequence number is *not used for reassembly* because "the Layer 2 receiving portion … expects to receive the segments (packets) in sequence." JX-1 at col. 4, lns. 53-55; Acampora Tr. 790-791 ("There may be no resequencing. The packets may have arrived in order."), 792. Terms should not be construed to exclude disclosed embodiments. *Oatey Co. v. IPS Corp.*, 514 F. 3d 1271, 1276 (Fed. Cir. 2008) ("We normally do not interpret claim terms in a way that excludes embodiments disclosed in the specification").

In addition, non-asserted claim 5 element (j) of the '712 patent specifically requires that the sequence number be used to reorder the received packets. JX-1 at col. 6, ln. 53 to col. 7, ln. 34. The basic rule of claim differentiation dictates that Microsoft's attempt to read limitations of claim 5 into the asserted claims is improper. *Karlin Tech.*, 177 F.3d at 971-72.

5. " assigning a packet sequence number to a packet derived from a data stream received from the network layer" (claims 6 and 17)

Claim Term	Motorola's Proposed Construction	Microsoft's Proposed Construction
"assigning a packet sequence number to a packet derived from a data stream received from the network layer" (claims 6 and 17)	assigning a packet sequence number to a packet formed or developed from a data stream received from the network layer	assigning a "packet sequence number" to a "packet" created by segmenting a "data stream" received from the network layer

The claim term "assigning a packet sequence number to a packet derived from a data stream received from the network layer" appears in element (a) of independent apparatus claim 6 and independent method claim 17. JX-1.[87]

Motorola construes the term to mean "assigning a packet sequence number to a packet formed or developed from a data stream received from the network layer." Compls. Br. at 213. Microsoft construes the term to mean "assigning a 'packet sequence number' to a 'packet' created by segmenting a 'data stream' received from the network layer." Resp. Br. at 19.

As proposed by Motorola, the claim term "assigning a packet sequence number to a packet derived from a data stream received from the network layer" is construed to mean "assigning a packet sequence number to a packet formed or developed from a data stream received from the network layer."

Motorola's proposed definition is consistent with the claim language, only elaborating on the word "derived" as used in its ordinary English language sense: "formed or developed out of something else," *i.e.*, the packet is formed or developed

[87] The term also appears in non-asserted claims. JX-1.

from the data stream received from the network layer. *See* CX-371, Webster's Third New International Dictionary (Unabridged) (2002); CX-708C (Acampora WS) at 75. Microsoft asserts that the patentee intended to limit the term "derived from" to mean "segmenting." RRX-24C (Housley RWS) at 31. Microsoft points to the use of the word "segment" in the specification and argues that the patentee meant to use it to be synonymous with the claim term "derived." RRX-24C (Housley 31). But, as the Federal Circuit recently held, for a patentee to redefine a term from its plain and ordinary meaning, "[i]t is not enough for [the] patentee to simply disclose a single embodiment or use a word in the same manner in all embodiments, the patentee must "clearly express an intent" to redefine the term." *Thorner v. Sony Computer Entm't*, 2012 WL 280657 at *2 (Fed. Cir. 2012).

"Segmenting" is not a requirement of the asserted claims. Housley Tr. 1399 (noting that "segmenting" does not appear in the asserted claims); Acampora Tr. 983-986. Significantly, claim 5, which is not asserted, specifically requires "segmenting a data stream … into a plurality of packets" before the limitation of "assigning a packet sequence number …." Housley Tr. 1401-1402 (noting that "segmenting" appears in claim 5); Acampora Tr. 987. Again, as discussed, claim differentiation dictates that Microsoft's construction is unsound. There is no reason, for example, why the data stream received from Layer 3, the Network Layer, cannot already be segmented, rendering it unnecessary to further segment that data in Layer 2. The OSI standard specifically provides for segmenting in Layer 3. CX-369 at 44-45. Indeed, Mr. Housley agreed that segmenting can occur in OSI layer 3. Housley Tr. 1404; 1407-1408; Acampora Tr. 834.

Microsoft attempts to support its segmentation argument by referring to the language in this claim element, "derived from a data stream." RRX-24C (Housley RWS) at 26. Microsoft argues that this is part of the function performed by the assigning means structure. Microsoft is mistaken. This language specifies the source of the packet. The actual function performed by the assigning means is simply assigning a packet sequence number to that packet. CX-708C (Acampora WS) at 75.

6. "data stream" (claims 6 and 17)

Claim Term	Motorola's Proposed Construction	Microsoft's Proposed Construction
"data stream" (claims 6 and 17)	*No construction necessary.* *If construed:* a flow of data	non-packetized data

The claim term "data stream" appears in the preamble and element (a), of independent apparatus claim 6, and of independent method claim 17. JX-1.[88]

Motorola argues that no construction is necessary for this claim term. In the alternative, Motorola construes the term to mean "a flow of data." Compls. Br. at 214. Microsoft construes the term to mean "non-packetized data." Resp. Br. at 28.

The administrative law judge agrees with Motorola that the claim term "data stream" need not be construed.

Indeed, Microsoft appears to agree that no construction is necessary for this claim term. Resp. Br. at 28 ("Motorola insists on construing this term, although Microsoft does not belief that infringement turns on the construction of this term."). Curiously, however, Microsoft also proposes the term to mean "non-packetized data."

[88] The term also appears in non-asserted claims. JX-1.

In any event, the claim term "data stream" carries its plain and ordinary connoting a stream of data.

Microsoft's proposed construction is misguided. Microsoft is under the misimpression that the data stream that comes from the Network Layer in the preferred embodiment must be non-packetized. RRX-24C (Housley RWS) at 29. Microsoft presumably bases this misimpression on the fact that, in the preferred embodiment, the data stream from Layer 3 is segmented into packets after it is received by Layer 2. JX-1 at col. 3, lns. 62-64. Microsoft thus attempts to import this aspect of the preferred embodiment into its construction of data stream. However, as discussed in the previous section, the asserted claims do not require segmentation in Layer 2, and thus Microsoft's construction of "data stream" is rejected.

7. "updating means" (claim 6)

Claim Term	Motorola's Proposed Construction	Microsoft's Proposed Construction
"updating means" (claim 6) *Function*	*Function:* updating a transmit overflow sequence number as a function of the packet sequence number	
"updating means" (claim 6) *Structure*	*Structure:* overflow counter (124)	*Structure: This term is indefinite because the corresponding structure is not sufficiently described in the specification*

The claim term "updating means" appears in elements (b) and (c) of independent apparatus claim 6. JX-1.[89]

Both parties construe the function of the term to mean "updating a transmit

[89] The term also appears in non-asserted claims. JX-1.

overflow sequence number as a function of the packet sequence number."

Motorola construes the structure of the term to mean "overflow counter (124)." Compls. Br. at 216. Microsoft argues that this term is indefinite because the corresponding structure is not sufficiently described in the specification. Resp. Br. at 24.

As proposed by both parties, the function of the claim term "updating means" is construed to mean "updating a transmit overflow sequence number as a function of the packet sequence number."

As proposed by Motorola, the structure of the claim term "updating means" is construed to mean "overflow counter (124)."

Microsoft's assertion that this element is indefinite because there is insufficient disclosure of structure fails. RRX-24C (Housley RWS) at 33. Microsoft's expert agrees that the structure explicitly disclosed for the updating means is the overflow counter (124). Housley Tr. 1409–10. FIG. 1 discloses an overflow counter (124) that is updated when the packet sequence rolls over. JX-1, FIG. 1. "When SN 116 rolls over (*e.g.*, indicated by an overflow signal 122), the 24 bit long overflow counter 124 is incremented." JX-1 at col. 3, lns. 66-68. As discussed above in Section II.H.2(b), counters are common, well known components that can be implemented in hardware and/or software. CX-708C (Acampora WS) at 76. Given disclosure of a well-known electronic component, the requirements of Section 112(6) are satisfied. CX-708C (Acampora WS) at 81.

8. "transmit overflow sequence number" (claims 6 and 17)

Claim Term	Motorola's Proposed Construction	Microsoft's Proposed Construction

"transmit overflow sequence number" (claims 6 and 17)	*No construction necessary.* *If construed:* a finite multi-bit incrementing number that updates when the packet sequence number rolls over	a multi-bit number that counts the number of times that a "packet sequence number" rolls over, which is used in the transmitter but is not transmitted to the receive unit

The term "transmit overflow sequence number" appears in elements (b) and (c), of independent apparatus claim 6, and of independent method claim 17. JX-1.[90]

Motorola construes the term to mean "a finite multi-bit incrementing number that updates when the packet sequence number rolls over." Compls. Br. at 217. Microsoft construes the term to mean "a multi-bit number that counts the number of times that a 'packet sequence number' rolls over, which is used in the transmitter but is not transmitted to the receive unit." Resp. Br. at 13.

As proposed by Microsoft, the claim term "transmit overflow sequence number" is construed to mean "a multi-bit number that counts the number of times that a 'packet sequence number' rolls over, which is used in the transmitter but is not transmitted to the receive unit."

Properly construed, the transmit overflow sequence number cannot be sent to the receiver. Motorola's construction should be rejected because (1) the intrinsic evidence expressly requires a "transmit" overflow sequence number, not just an "overflow" sequence number, and the patent solely, and repeatedly, indicates the number is not transmitted; (2) its inventors, during prosecution to secure allowance of nearly identical claims, unequivocally characterized their invention as not transmitting this number; (3) one of the inventors, during litigation, indicated the number is not sent in order to

[90] The term also appears in non-asserted claims. JX-1.

enhance security; (4) Judge Crabb rejected Motorola's construction; (5) Judge Posner rejected Motorola's construction; and (6) Motorola's expert never considered the inventors' characterizations of the invention during prosecution in Japan, and indeed, Motorola chose to not even provide these characterizations to Motorola's expert.

Microsoft's construction of "transmit overflow sequence number" as a number that is not sent to the receiver is correct. The asserted claims do not require just any "overflow sequence number" – they require a "transmit overflow sequence number." JX-1 at col. 7, lns. 44-47; col. 9, lns. 5-6. Indeed, Motorola concedes that, in claim 1, the "transmit" overflow sequence number is not sent to the receiver.

> Motorola distinguished the invention of claim 1 on several grounds, including the fact that the overflow sequence number is not transmitted. *This is a correct statement for claim 1.*

337-TA-752, Motion 752-025, 2011 WL 6819246, at *9 (Nov. 28, 2011) (emphasis added). A term that is used in several claims is presumed to have the same meaning across all claims. *See Georgia Pacific Corp. v. United States Gypsum Co.*, 195 F.3d 1322, 1331 (Fed. Cir. 2000).

In addition, claims 11 and 18, which are both directed to the receiver, recite "updating a *receive* overflow sequence number" after "extracting a packet sequence number from the physical layer." JX-1 at col. 8, lns. 19-24 (emphasis added); col. 10; lns. 5-8 (emphasis added). The receive overflow sequence number is created in the receiver based on the packet sequence number because only the packet sequence number is transmitted; the transmit overflow sequence number is not. Acampora Tr. 795-796; RRX-24C (Housley RWS) at 35-37. In fact, *asserted* claims 6 and 17 only recite

transmitting the packet sequence number, not the transmit overflow sequence number. JX-1 at col. 7, lns. 49-51; col. 9, lns. 7-9. The patent claims recite three different elements, the "packet sequence number," the "transmit overflow sequence number" and the "receive overflow sequence number," each with its own distinct characteristics: the packet sequence number is transmitted; the transmit overflow sequence number is not, and the receive overflow sequence number is updated based on the received packet sequence number.

The specification also compels Microsoft's construction. FIG. 1, reproduced below, shows the transmitter 102 on the left and the receiver 104 on the right:

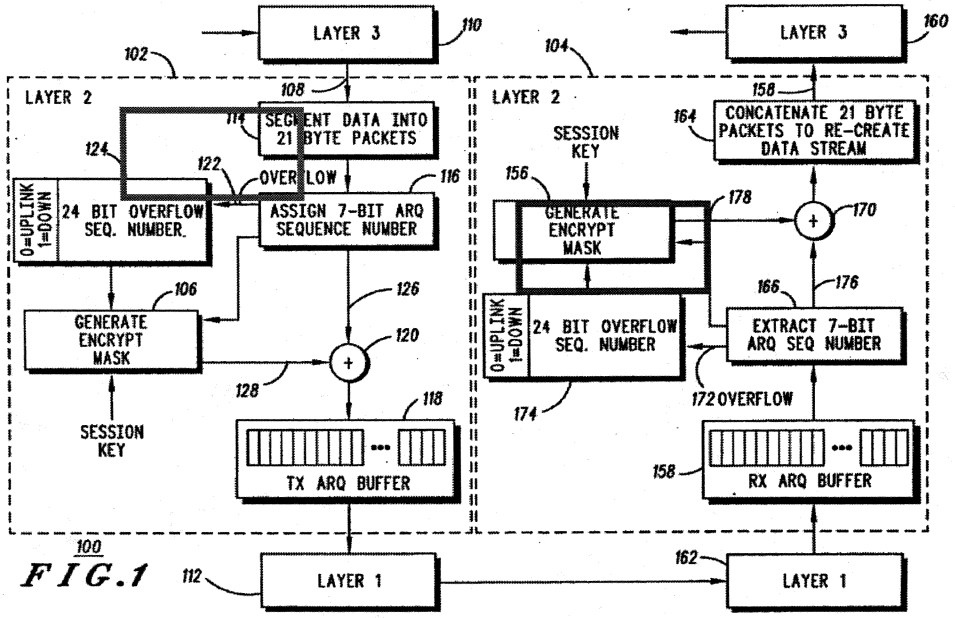


FIG. 1

The transmit overflow sequence number 124 (highlighted in green) used in the transmitter 102 is distinct from the receive overflow sequence number 174 (highlighted in red) used in the receiver 104. Rather than use a single "overflow sequence number," the specification consistently uses the term "transmit overflow sequence number" to refer to

the number in the transmitter (JX-1 at col. 2, lns. 27-29; col. 3, lns. 65-68; col. 5, lns. 17-19), as opposed to the "receive overflow sequence number" which is consistently described as being calculated by the receiver from the received packet sequence number. JX-1 at col. 2, lns. 35-37; col. 4, lns. 14-17; col. 5, lns. 41-43; RRX-24C (Housley RWS) at 35-37. Critically, Motorola's expert concedes that the transmit overflow sequence number is not transmitted in Figure 1:

> A. … the description of figure 1 does not include in this preferred embodiment the accompanying transmission of the transmit overflow sequence number. I agree with that.
> …
>
> Q. … Answer: In figure 1, the transmit overflow sequence number is not transmitted; that's correct."
>
> A. That's what I just said, yes.

Acampora Tr. 785. Acampora acknowledged that there is no disclosure in the specification that the transmit overflow sequence number is ever transmitted. Indeed, the only portion of the patent specification that he could point to in support of Motorola's position is the boilerplate language at "column 5, beginning line 55." *Id.* 812-813; JX-1 at col. 5, lns. 55-65. But there is no mention of transmitting the number in this passage. Acampora Tr. 813-818.

The inventors made very clear that the claimed "transmit overflow sequence number" is *never* transmitted to the receiver. Specifically, in response to a Japanese Office Action rejecting the application, which contained claims identical in substance to

claims 6 and 17,[91] Motorola argued:

> Additionally, the aforementioned overflow sequence numbers are absolutely not communicated to the ends of the communication route, they are not embedded in the data packets, nor may they be deduced from data embedded in the data packets. The aforementioned overflow sequence numbers are determined independently by both the communication device for transmission and the communication device for reception. Unlike keys, or unlike the packet sequence numbers, there is no danger of interception of the overflow sequence numbers, and they provide an even higher level of security.
>
> Therefore, using packet sequence numbers and overflow sequence numbers for encrypting/decoding data could not have easily been thought of by one skilled in the art based on the aforementioned cited example, and it is clear that they are not simply one selection of the many variables used as keys. Therefore, the invention described in Claim 1, and in Claims 2-4 that are dependent on said Claim 1, in the application clearly could not easily have been invented by one skilled in the art based on the aforementioned cited example.

RX-343 at 0019 (emphases added). Contrary to Motorola's contention that its statements do not apply to the claims at issue here, Motorola represented to the Japanese government:

> Additionally, Claims 5, 7, 9 and 10 of the application also provide encryption/decoding technology that uses packet sequence numbers and communication overflow sequence numbers, in addition to session keys, for encrypting/decoding data. Therefore, for the same reasons as stated above, we think that the inventions described in these claims also could not easily have been invented by one skilled in the art based on the aforementioned cited example.

---

[91] Claims 5 and 9 of the Japanese Application are substantively identical to asserted claims 6 and 17 of the '712 patent, respectively. *See* RX-343 at 0025-27. While there are slight differences in the wording of the claims of the Japanese Application and the claims of the '712 patent, these differences do not affect the substance of the claims.

RX-343 at 0019 (emphases added). Then, during appeal proceedings, Motorola again argued that the overflow sequence number is not sent to the receiver and explained the benefits of not transmitting it:

> The invention in the application relates to a method and communication devices to provide protection using data stream ciphers in a communication system that has a physical layer, a data link layer, and a network layer. It is characterized by the fact that, by using overflow sequence numbers that are not sent from one end of the communication route to the other end, the communication device for reception and the communication device for transmission can each independently execute an algorithm for the overflow sequence numbers, independently of the output of the algorithm executed by the other communication device, and without knowing that output.

RX-343 at 0051 (emphases added).

* * *

> … the applicant stated that in the invention in this application, the overflow sequence numbers are determined based on rollover of the packet sequence numbers, the overflow sequence numbers are determined and maintained internally in each device, and are not communicated outside of either device, and interception can therefore be prevented. That is, even if a specific packet is intercepted, the overflow sequence numbers used for encrypting and decoding the packet cannot be detected. The overflow sequence numbers are absolutely not embedded in the packets, and unless the sequence number rolls over, the packet sequence number will not be deduced from other data in a specific packet (singular or multiple).

RX-343 at 0051-52 (emphases added).

Inventor Finkelstein agreed that not sending the transmit overflow sequence number enhances security:

> A. In this particular embodiment you have the seven bits of the sequence number that go over the – over the

> physical link. So they're in some sense available. But the other information is not. The overflow number is not. And therefore, that's more secretive – more unknown information at the time going to the encryption algorithm that generated the encryption mask.
>
> And that – that means that somebody would have to in some sense guess what – what the overflow sequence number is as opposed to being given it.

RX-185C at 0029-30. Motorola cannot rely on one position to obtain a patent and take the opposite position in litigation.

Further, two courts have fully considered the record and held that the transmit overflow sequence number is not sent. Judge Crabb in the Western District of Wisconsin rendered a Markman decision, holding that "the overflow sequence number is never transmitted to the receiver." RRX-72 at 0022-30 (*Apple, Inc. v. Motorola, Inc.*, 3:10-cv-662-bbc (WD Wis. Oct. 13, 2011)). As Judge Crabb explained, "[Motorola] made statements confirming that it designed the claimed method of the '712 patent to exclude transmission of the transmit overflow sequence number in order to increase the efficiency and security of transmission." RRX-72 at 0024-25. After the case was transferred to the Northern District of Illinois, Judge Posner fully considered the record, adopted Judge Crabb's construction, and rendered summary judgment of non-infringement of Apple's WPA-based products. RRX-116 at 1-3 (*Apple, Inc. v. Motorola, Inc.*, 1:11-cv-08540 (ND Ill. Jan. 16, 2012)). Judge Posner held that the accused WPA products do not infringe Motorola's '712 patent because "the extended initialization value in WPA is transmitted (and it is the only structure that is potentially analogous to the patented transmit overflow sequence number)." RRX-116 at 2. Judge Posner explained:

"Motorola told that office that 'unlike the key or the packet sequence number, there is no chance to intercept the overflow sequence number [a reference to the "transmit overflow sequence number" in the '712 patent]; thus it provides a higher level of security' – no chance because that number is never transmitted, unlike its counterpart in Apple's devices that are alleged to infringe." RRX-116 at 2.[92] Further, despite being aware of the Japanese foreign prosecution from two separate litigations, Motorola did not provide these documents to Dr. Acampora.

9. "encrypting means" (claims 6 and 8)

Claim Term	Motorola's Proposed Construction	Microsoft's Proposed Construction
"encrypting means" (claims 6 and 8) *Function*	*Function:* encrypting ... the packet as a function of the packet sequence number and the transmit overflow sequence number	
"encrypting means" (claims 6 and 8) *Structure*	*Structure:* exclusive-or operator (120)	*Structure: This term is indefinite because the corresponding structure is not sufficiently described in the specification.* *In the alternative, the corresponding structure is:* an exclusive-or operator (120) with a pseudo-random bit generator (106).

The claim term "encrypting means" appears in element (c) of independent apparatus claim 6, and in dependent claim 8. JX-1.

Both parties construe the function of the term to mean "encrypting ... the packet

[92] The WD Wis. Markman and ND Ill. summary judgment decisions were rendered after Motorola had a full and fair opportunity to litigate the construction it presents here. Courts have found collateral estoppel under similar circumstances. *See Certain Electronic Devices with Multi-touch Enabled Touchpads and Touchscreens*, 337-TA-714, Order No. 16 at 3 (Sept. 28, 2010) (Initial Determination Finding Complainant Collaterally Estopped From Certain Pleadings).

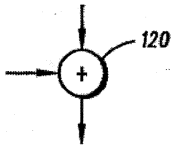
as a function of the packet sequence number and the transmit overflow sequence number."

Motorola construes the structure of the term to mean "exclusive-or operator (120)." Compls. Br. at 225. Microsoft argues that this term is indefinite because the corresponding structure is not sufficiently described in the specification. In the alternative, Microsoft construes the structure of the term to mean "an exclusive-or operator (120) with a pseudo-random bit generator (106)." Resp. Br. at 21.

As proposed by both parties, the function of the claim term "encrypting means" is construed to mean "encrypting ... the packet as a function of the packet sequence number and the transmit overflow sequence number."

As proposed by Motorola, the structure of the claim term "encrypting means" is construed to mean "exclusive-or operator (120)."

Microsoft is wrong in both facets of its two-pronged construction. The '712 patent explicitly discloses structure, the exclusive-or operator (120), for performing this function. CX-708C (Acampora WS) at 83. As disclosed at column 3, lines 59-61, the patent unambiguously states that "encipherment (120) is performed (*e.g.*, an exclusive-or operation of the packetized data stream 126 with the encryption mask 128) on [the data]." *See also* JX-1 ('712 patent), col. 4, lns. 5-6 ("encryption 120"), col. 5, ln. 24 ("encrypted 120"). In addition, Figure 1 of the patent explicitly depicts the structure 120 that performs the XOR operation as the XOR gate symbol. There is no dispute that the XOR gate is a well-known structure.



Microsoft's alternative position that the encrypting means is the pseudo-random bit generator 106 *plus* the exclusive-or operator 120 also fails. The specification

identifies *only* the XOR operation as "encryption 120" or "encipherment 120." JX-1 ('712 patent), col. 3, ln. 59, col. 4, lns. 5-6, col. 5, ln. 24. If the patent intended to include more than the exclusive OR operator, the term "encryption" or "encipherment" would not have been used solely to describe exclusive-or 120.

Moreover, the pseudo-random bit generator is not used to perform the claimed function of "encrypting." Rather this component performs the unclaimed act of generating an encrypt mask, *which occurs prior* to encryption and is used as an *input* by the structure that actually performs the encryption, the exclusive-or operator. JX-1 ('712 patent) at col. 3, lns. 32-38; CX-708C (Acampora WS) at 32-33. Because the pseudo-random bit generator is not necessary for performing the claimed function, but merely generates an input to the structure that performs the function, it should not be included in the claimed structure. *See Asyst Techs., Inc. v. Empak, Inc.*, 268 F.3d 1364, 1370-1371 (Fed. Cir. 2001) (finding communication cable not corresponding structure because it did not actually perform the functions of "controlling" and "transmitting," despite the fact that it conveyed the information to be "controlled" and "transmitted").

In any event, whether the corresponding structure is the exclusive-or operator (120) alone, or coupled with a pseudo-random bit generator, the requirements of Section 112(6) are satisfied. Exclusive-or operators and pseudo-random bit generators are well known electronic components, and can be implemented in hardware or software in well known, standard ways. Housley Tr. 1367-69, 1419-1420; Acampora Tr. 840-841 ("[O]ne of skill in the art would know that … any of many known algorithms that accept some inputs could have been used."); CX-708C (Acampora WS) at 34. *See Atmel Corp.*, 198 F.3d at 1379-80 (stating that disclosed structure may be implicit in patent's written

description if clear to a person of ordinary skill in the art); *Creo Prods.*, 305 F.3d at 1347.

B. Infringement Analysis of the '712 Patent

Microsoft argues that Motorola has failed to show that anyone has ever performed the method steps of claim 17 of the '712 patent. Resp. Br. at 10. According to Microsoft, it is not enough to show that a particular article is capable of performing the claimed steps; instead, the patentee must show that each step is actually performed in the United States. *Id.* citing *Joy Techs.*, 6 F.3d at 775. Microsoft's argument is rejected.

As is the case for the '571 patent, *supra*, Motorola's infringement claims for the '712 patent are based, in part, on the Xbox's implementation of the IEEE's 802.11 Wi-Fi standard, and the normal use of the Xbox with Wi-Fi in a home environment. CX-708C (Acampora WS) at 86-95, 182-83 As discussed above for the '571 patent, the record establishes that the Xbox products are compliant with the IEEE 802.11 standard, and that the 802.11-2007 standards document (CX-383) describes the Xbox for the purposes pertinent to this investigation. *Id.*; RX-314C at 8; Housley Tr. 1345-1346.

1. Accused Products

Motorola argues that the accused products are Microsoft's Xbox 360 console, including the Xbox 360 S 4 GB and 250 GB consoles, as well as the Xbox 360 Wireless N Adapter (collectively, "the Xbox"), imported into the United States, and/or sold after importation. Compls. Br. at 226-27 citing CX-708C (Acampora WS) at 86 and Tab E.

Microsoft argues that Motorola failed to provide any evidence that the accused products that contain Atheros chips infringe the '712 patent. Resp. Br. at 8-10.

In connection with the accused products for the '571 patent, *supra*, the undersigned found that Microsoft is precluded from arguing that Xbox products containing [ ] chips should be determined to be non-infringing. For the same reasons, the administrative law judge is not making any factual findings on whether Xbox products containing [ ] chips are non-infringing.

2. Direct Infringement

For the reasons set forth below, Motorola has not shown that Microsoft's accused products directly infringe all asserted claims of the '712 patent.

Claim 6

The preamble of independent apparatus claim 6 recites:

> **A transmitting communication unit for providing cryptographic protection of a data stream in a communication system having a physical layer, data link layer, and a network layer, transmitting communication unit comprising a data link layer device having:**

Motorola has established that this claim limitation is satisfied.

The Xbox literally infringes the preamble of claim 6. When communicating with a router set for WPA/TKIP security, the Xbox is a transmitting communication unit. CX-708C (Acampora WS) at 187. Per 802.11, the Xbox and router are part of a communication system having physical, data link, and network layers. CX-708C (Acampora WS) at 98, 187-88; CX-383 at Section 5.7 ("This standard presents the architectural view, emphasizing the separation of the system into two major parts: the MAC of the data link layer (DLL) and the PHY."); Acampora Tr. 746. The data link layer (*i.e.*, the upper boundary of the 802.11 LLC) interfaces with Layer 3 of the OSI

model and accepts Layer 3 formatted information. CX-393C; CX-656C (Lambert Dep. Tr.) at 111-12; CX-400C. Microsoft's expert, Mr. Housley, admits that TKIP occurs in layer 2. Housley Tr. 1379.

The first element of claim 6 recites:

> **(a) assigning means for assigning a packet sequence number to a packet derived from a data stream received from the network layer;**

Motorola has established that this claim limitation is satisfied.

As proposed by both parties, the function of the claim term "assigning means" has been construed to mean "assigning a packet sequence number to a packet derived from a data stream received from the network layer." As proposed by Motorola, the claim term "packet sequence number" has been construed to mean "a multi-bit incrementing number that is transmitted along with the 'packet'." As proposed by Motorola, the structure of the claim term "assigning means" has been construed to mean "a counter and related structure (116) implemented in hardware and/or software." As proposed by Motorola, the claim term "assigning a packet sequence number to a packet derived from a data stream received from the network layer" has been construed to mean "assigning a packet sequence number to a packet formed or developed from a data stream received from the network layer."

The Xbox literally infringes this element. Per 802.11, when using TKIP, data packets called MPDUs (MAC Protocol Data Units) derived from a data stream received from the network layer are provided to the Xbox's Wi-Fi chip. CX-708C (Acampora WS) at 189. The chip generates a 2-byte sequential count, comprising "TSC0" and "TSC1," which increments for each MPDU. *Id.* at 189-90; Housley Tr. 1386-89. This is