NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

2006-1603

DATA ENCRYPTION CORPORATION,

Plaintiff/Counterclaim Defendant-Appellant,

v.

MICROSOFT CORPORATION,

Defendant/Counterclaimant-Appellee,

and

DELL COMPUTER CORPORATION,

Defendant-Appellee.

Roderick G. Dorman, Hennigan, Bennett & Dormann LLP, of Los Angeles, California, argued for plaintiff/counterclaimant defendant-appellant. With him on the brief were Lawrence M. Hadley, Bless S. Young, and Hazim H. Ansari.

Kelly C. Hunsaker, Fish & Richardson P.C., of Redwood City, California, argued for defendant/counterclaimant-appellee. With him on the brief for Microsoft Corporation were Juanita R. Brooks and William Chad Shear, of San Diego, California. Of counsel was Robert B. Lytle, Microsoft Corporation, of Redmond, Washington.

Daniel T. Conrad, Jones Day, of Dallas Texas, argued for defendant-appellee. With him on the brief for Dell Computer Corporation was Mark N. Reiter. Of counsel was Amy E. Blackwelder.

Appealed from: United States District Court for the Central District of California

Judge Manuel L. Real

NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

2006-1603

DATA ENCRYPTION CORPORATION,

Plaintiff/Counterclaim Defendant-Appellant,

v.

MICROSOFT CORPORATION,

Defendant/Counterclaimant-Appellee,

and

DELL COMPUTER CORPORATION,

Defendant-Appellee.

DECIDED: September 6, 2007

Before RADER, BRYSON, and PROST, Circuit Judges.

PROST, Circuit Judge.

Plaintiff-Appellant, Data Encryption Corporation ("Data") appeals the decision of the United States District Court for the Central District of California granting summary judgment of noninfringement of U.S. Patent No. 5,584,023 (the "'023 patent") in favor of Defendants-Appellees, Microsoft Corporation ("Microsoft") and Dell Computer

Corporation ("Dell"). Data Encryption Corp. v. Microsoft Computer Corp., No. 05-CV-05531 (C.D. Cal. Aug. 14, 2006). We affirm.

I. BACKGROUND

Data is the owner of the '023 patent, entitled "Computer System Including a Transparent and Secure File Transform Mechanism." Generally speaking, the '023 patent is directed to computer systems that encrypt and decrypt files. On July 29, 2005, Data sued Microsoft and Dell, alleging that Microsoft's Windows operating systems and Dell computers using Windows operating systems infringed claims 5-12 of the '023 patent.

The parties filed cross motions for summary judgment. On August 14, 2006, the district court (1) granted Microsoft's motion for summary judgment of noninfringement, (2) granted Dell's motion for summary judgment of noninfringement, and (3) denied Data's motion for partial summary judgment of infringement of claims 5, 6, and 7 by Microsoft and Dell.

Data appeals. We have jurisdiction under 28 U.S.C. § 1295(a)(1).

II. DISCUSSION

A

On appeal, Data argues that the district court misconstrued the asserted claims and that, therefore, the district court's infringement analysis was incorrect. We review the district court's claim construction de novo. Cybor Corp. v. FAS Techs., Inc., 138 F.3d 1448, 1456 (Fed. Cir. 1998) (en banc). We also review de novo the district court's grant of summary judgment of noninfringement. O2 Micro Int'l Ltd. v. Monolithic Power Sys., Inc., 467 F.3d 1355, 1369 (Fed. Cir. 2006).

Of the asserted claims, claims 5 and 8 are independent. Claim 5 recites:[1]

5. A computer system including a file encryption mechanism, said system comprising:

a) a file store providing for the storage of a file including one or more blocks of data;

b) a memory store providing for the storage of blocks of data in first and second logical data areas; and

c) a processor coupled to said memory store and said file store for executing instructions implementing a computer operating system as stored in said first logical data area and an application program as stored in said second logical data area, said processor providing for the controlled transfer of a predetermined block of data between said file store and said data store means, said processor including:

i) an encryption routine, defined by the execution of instructions of said computer operating system, for encrypting and decrypting said predetermined block of data in said first logical data area separately from another block of data;

ii) a request routine, defined by the execution of instructions of said application program, for selecting said predetermined block of data to be operated on by the execution of instructions of said application program in said second logical data area; and

iii) a system interface routine, defined by the execution of instructions of said computer operating system and responsive to said request routine, that controls the transfer of said predetermined block of data between said file store and said data store and between said first and second logical data areas of said data store, said system interface routine determining whether said predetermined block of data is encrypted as stored by said file store, said system interface routine selectively directing the transfer of said predetermined block of data between said first and second logical data areas through said encryption routine.

(Emphases added). The parties agreed before the district court that the term "first logical data area" as recited in the claim refers to the kernel memory area and that the term "second logical data area" refers to the user memory area.

[1] On appeal, Data presents no separate argument regarding independent claim 8. We therefore discuss only independent claim 5.

In granting summary judgment of noninfringement, the district court held that certain statements in the specification amounted to a disavowal of coverage of systems that maintain data subject to encryption in an unencrypted state in the kernel memory buffer pool, or cache. Data Encryption Corp. v. Microsoft Computer Corp., No. 05-CV-05531, slip op. at 2 (C.D. Cal. Aug. 14, 2006) (order granting Microsoft's motion for summary judgment). The court further held that the phrase "system interface routine selectively directing the transfer of said predetermined block of data between said first and second logical data areas through said encryption routine" requires that "the encryption routine in kernel memory transforms (i.e., encrypts or decrypts) the data in user memory when it is transferred between kernel memory and user memory, not when it is transferred between memory and the disk." Id. In light of its interpretation, the court concluded that there was no genuine dispute as to any material fact that Microsoft Windows products did not infringe any of the asserted claims and, accordingly, granted summary judgment to Microsoft and Dell. Id., slip op. at 2-3; Data Encryption Corp. v. Microsoft Computer Corp., No. 05-CV-05531, slip op. at 2 (C.D. Cal. Aug. 14, 2006) (order granting Dell's motion for summary judgment).

B

At issue is the proper construction of the phrase "system interface routine selectively directing the transfer of said predetermined block of data between said first and second logical data areas through said encryption routine." Data argues that the district court incorrectly concluded that the inventor disavowed coverage of systems that maintain data subject to encryption in an unencrypted state in the kernel memory buffer pool.

We agree with the district court that the specification reveals a disavowal of claim scope. See Phillips v. AWH Corp., 415 F.3d 1303, 1316 (Fed. Cir. 2005) (en banc) ([T]he specification may reveal an intentional disclaimer, or disavowal, of claim scope by the inventor. In that instance . . ., the inventor has dictated the correct claim scope, and the inventor's intention, as expressed in the specification, is regarded as dispositive."). The '023 patent specification explains that, in accordance with the invention,

> data pending either a read or write operation to disk 22 or other storage medium persists only in an encrypted state. All data subject to encryption by operation of the present invention is maintained in an encrypted state in the buffer pool.[2]

'023 patent, col. 14, ll. 10-14 (emphasis added). This language is unambiguous. By stating that "[a]ll data subject to encryption by operation of the present invention is maintained in an encrypted state in the [kernel memory] buffer pool," the inventor has disavowed coverage of systems that maintain data subject to encryption in an unencrypted state in the kernel memory buffer pool.

Data nevertheless asserts that the above-quoted language should not inform the construction of claim 5—and should therefore not amount to a disavowal of claim scope—because claim 5 makes no mention of how data is "maintained" in the kernel memory buffer pool. While it is true that claim 5 makes no mention of how data is maintained in the kernel memory buffer pool, it is also true that claim 5 specifies that the system decrypts data when it is transferred from the kernel memory to the user memory. Specifically, claim 5 requires the system to "selectively direct[] the transfer of said predetermined block of data between said first and second logical data areas[, i.e.,

[2] The buffer pool is located within the kernel memory area. See '023 patent, col. 5, ll. 63-64 ("Within the kernel space, a buffer pool, or buffer cache, is maintained by the operating system.").

between the kernel memory and the user memory,] through said encryption routine." Thus, the specification's statement that "[a]ll data subject to encryption by operation of the present invention is maintained in an encrypted state in the [kernel memory] buffer pool" is clearly relevant to claim 5's requirement that data be decrypted upon its transfer from the kernel memory to the user memory.

In light of the inventor's disavowal of claim scope, we affirm the district court's grant of summary judgment of noninfringement. Data does not dispute that, in normal operation, Windows operating systems maintain data subject to encryption in an unencrypted state in the kernel memory buffer pool, or cache.

Notwithstanding the disavowal, Data argues that there is a genuine issue of material fact regarding infringement by operation of Windows operating systems in non-default mode. We have carefully examined Data's arguments in this regard and find them to be unpersuasive. We similarly find unpersuasive Data's contention that the district court erroneously denied its motion for further discovery pursuant to Federal Rule of Civil Procedure 56(f).

III. CONCLUSION

For the above reasons, we affirm the district court's judgment of noninfringement.