United States Court of Appeals for the Federal Circuit

04-1129, 04-1147, 04-1148

LEON STAMBLER,

Plaintiff- Appellant,

v.

RSA SECURITY, INC.,

Defendant-Cross Appellant,

and

VERISIGN, INC.,

Defendant-Cross Appellant.

DECIDED: February 11, 2005

Before RADER, Circuit Judge, ARCHER, Senior Circuit Judge, and BRYSON, Circuit Judge.

ARCHER, Senior Circuit Judge.

Leon Stambler ("Stambler") appeals the judgment of the United States District Court for the District of Delaware denying his motion for judgment as a matter of law ("JMOL") or, in the alternative, for a new trial. Contrary to Stambler's argument, RSA Security, Inc. and VeriSign, Inc. ("RSA") did not argue to the jury a construction of claim 34 of U.S. Patent No. 5,793,302 ("the '302 patent") counter to that set forth by the district court. As discussed below, we conclude 1) substantial evidence supports the jury's noninfringement verdict; 2) Stambler did not show that defense counsel

improperly influenced the jury; and 3) the district court did not abuse its discretion in bifurcating the issues of validity and infringement. Accordingly, we affirm the judgment of the district court. Stambler v. RSA Security, No. 01-0065-SLR (D. Del. 2003).

Background

Stambler sued RSA for, inter alia, infringement of the '302 patent based on its use of Secure Sockets Layer version 3.0 ("SSL 3.0"). The patented methods enable parties to a transaction to assure the identity of an absent party and the accuracy of information involved in the transaction, thus providing for secure transactions and preventing fraud. Id. at 2. SSL 3.0 is widely considered to be the standard method for conducting secured communications via the Internet. Id. at 5. The SSL 3.0 protocol addresses two security issues pertaining to Internet communications. Id. The protocol insures that parties communicating over the Internet are certain of each other's identity and that communications between the parties cannot be intercepted and deciphered by an unauthorized party. Id.

Claim 34 of the '302 patent is at issue here. Claim 34 is dependent upon claim 33, which states the following:

> A method for authenticating a first party by using information stored in a credential, the credential being previously issued to the first party by a second party, wherein information previously stored in the credential comprises at least a non-secret variable authentication number (VAN) and other non-secret credential information, the method comprising:
> previously generating a first error detection code (EDC1) by using at least a portion of the other non-secret credential information;
> previously coding the first error detection code (EDC1) with first information associated with the second party to derive a variable authentication number (VAN);
> previously storing the VAN and the other non-secret credential information in the credential;
> retrieving the VAN and the other non-secret credential information stored in the credential;

> deriving a second error detection code (EDC2) by using at least a portion of the retrieved other non-secret credential information;
> retrieving second information associated with the second party previously stored in a storage means associated with at least one of the parties;
> uncoding the VAN using the second information associated with the second party to derive a third error detection code (EDC3);
> and authenticating the first party and at least a portion of the non-secret information stored in the credential if the second error detection code (EDC2) corresponds to the third error detection code (EDC3).

'302 patent, col. 30 ll. 35-65. Claim 34 states that it is a "method of claim 33 wherein the first information associated with the second party comprises a public key, and the second information associated with the second party comprises a non-secret key." Id. at col. 30, line 66 – col. 31, line 2.

Following a verdict of non-infringement, Stambler filed a renewed motion for JMOL and, in the alternative, for a new trial. The district court denied the motions, and Stambler now appeals. We have jurisdiction pursuant to 38 U.S.C. § 1295(a)(1).

Discussion

Stambler argues that the district court erred in denying his renewed motion for judgment as a matter of law because the district court permitted defendants to add limitations to the claim language. Stambler further asserts he should be accorded a new trial because defense counsel improperly influenced the jury and because bifurcation of the infringement and validity issues resulted in a fundamentally unfair trial in violation of his rights under the Seventh Amendment.

The denial of JMOL is reviewed without deference and reversed only if substantial evidence does not support a jury's factual findings or if the law cannot support the legal conclusions underpinning the jury's factual findings. Moba, B.V. v. Diamond Automation, Inc., 325 F.3d 1306, 1312 (Fed. Cir. 2003). The denial of a

motion for a new trial is reviewed under the abuse of discretion standard. Motorola, Inc. v. Interdigital Tech. Corp., 121 F.3d 1461, 1468 (Fed. Cir. 1997), as is the propriety of the district court's order bifurcating infringement and validity, Barr Labs., Inc. v. Abbott Labs., Inc., 978 F.2d 98, 105 (3d Cir. 1992).

Stambler argues that the district court erred in denying his renewed motion for judgment as a matter of law because, according to Stambler, it upheld the jury's verdict of non-infrignement based on a finding that it was "reasonable" for the jury to adopt additional claim limitations.

Experts from both sides offered testimony as to the three disputed limitations, "credential," "storage means associated with one of the parties," and "authenticating the first party." RSA's expert did not change the district court's claim construction as to any of these elements by adding further claim limitations. To the contrary, RSA's expert simply took the district court's claim construction and provided detailed testimony as to why the accused device did not meet the claim limitations.

For example, the district court construed "credential" to mean "a document or information obtained from a trusted source that is transferred or presented to establish the identity of a party." RSA's expert explained that SSL 3.0 does not possess a "credential" as construed by the district court because in SSL 3.0 when the credential is presented it does not verify a user's identity. This argument neither narrows nor is inconsistent with the district court's claim construction. Rather, it is a reasonable interpretation of the court's claim construction given that "establish" means "1. to bring into being on firm or permanent basis; found; . . . 3. to cause to be accepted or recognized. 4. to show to be valid or true." Random House Col. Dictionary 452

(revised ed. 1980). Therefore, we are not persuaded by Stambler's arguments that the district court permitted RSA to argue a position to the jury that added further claim limitations and was inconsistent with the court's claim construction.[1]

Stambler argues the digital certificate created by SSL 3.0 is a credential within the meaning of claim 34. However, as noted by the district court "a reasonable jury could have concluded that the digital certificate is not a credential . . ., because [it] could reasonably conclude that the identity of the website is not established in SSL 3.0 at the time the [digital certificate] is presented or transferred." Stambler, slip op at 13. Based on the record, including the testimony of RSA's expert, we conclude that substantial evidence supports the jury's verdict of non-infringement.[2]

Stambler asserts two grounds for granting him a new trial: defense counsel's "misconduct" of discussing independent development and dedication to the public prejudiced the jury against Stambler and the court's bifurcation of the validity and infringement issues.

Stambler argues that "from opening to close" a "false theme" was emphasized by RSA, namely, a finding of infringement would mean that the patent-in-suit covers work done by others and which was placed in the public domain and, therefore, is freely used today by millions of people on a daily basis. As such, a verdict in Stambler's favor would allow him to usurp that which had already been dedicated to the public. Stambler

---

[1] We note that our discussion of this issue presumes that RSA's expert's testimony was properly before the jury – an issue discussed at great length at oral argument. Stambler's counsel did not adequately object to this testimony at trial, and therefore, there is no basis for saying that the testimony was improperly before the jury.

[2] Because substantial evidence supports the finding that SSL 3.0 does not contain a "credential" as construed by the district court, we need not discuss the other disputed limitations, as a product must contain each and every limitation of a claim in order to infringe that claim.

contends that this "message" was highly improper and extremely prejudicial and, as a result, the court erred by finding that defense counsel's mention of these issues did not reach the threshold of misconduct requiring a new trial.

Any purported improper mention of the dedication to the public and independent invention issues was cured by the trial judge. Specifically, the judge stated

> Defendants have spoken in their opening statements about plaintiff's motivation in bringing the litigation and about the industry's response to the litigation. Those issues, if proven, may be relevant to the issue of damages should you reach that issue, but keep in mind that the question of infringement is the first and primary determination you will need to make. . . . And I also remind you that you cannot let sympathy or bias or other irrelevant matters interfere with your duty to impartially review the evidence consistent with my instructions of the law that you will receive at the end of the evidence.

Further, the jury instructions expressly included the following statement: "[e]vidence that SSL may have been developed through independent research is not relevant to the question of literal infringement. An independently developed product or process that falls within the scope of the asserted patent claims nevertheless infringes." A11466. Because we presume the jury follows the instructions provided by the district court, United States v. Hakim, 344 F.3d 324, 326 (3rd Cir. 2003), there is no reason to believe the jury improperly considered testimony related to independent development or public dedication in reaching its finding of noninfringement.

Accordingly, we agree with the district court that there was "not prejudice to [Stambler] of the quality and quantity that would demand the jury's verdict to be set aside." Stambler, slip op at 19.

Stambler's final contention is that he should receive a new trial based on the violation of his Seventh Amendment rights. The thrust of his argument is that he did not

receive a trial based solely on infringement because RSA was unable to separate issues of validity from infringement. The result was that "separate trial[s] allowed defendants to tarnish the validity of the patents-in-suit gratuitously during the infringement trial, freed from the presumption of validity and the burden of proving invalidity by clear and convincing evidence." As discussed above, the district court told the jury that the "first and primary" issue at trial was infringement, and the jury was specifically instructed that "[e]vidence that SSL may have been developed through independent research is not relevant to the question of literal infringement." Because there is nothing in the record to suggest that the jury was confused, we cannot say that the district court abused its discretion in bifurcating the invalidity and infringement aspects of the trial.

Because we discern no error in the district court's denial of Stambler's renewed motion for JMOL and his motion for a new trial, we affirm the judgment of the district court.