

EXHIBIT 5

Apple's Invalidation Contentions Under Patent Rule 3-3
 Exhibit D-14

INVALIDITY OF U.S. PATENT NO. 9,467,838 (the "838 patent")

by

FORCE XXI BATTLE COMMAND, BRIGADE AND BELOW ("FBCB2")

As explained in the cover pleading to Apple's invalidity contentions, Plaintiff has not and cannot demonstrate that the '838 patent is entitled to a priority date earlier than October 31, 2014, the effective filing date of Appl. No. 14/027,410. On information and belief, the FBCB2 system (including at least FBCB2 software versions 3.2, 3.3, and 3.4 and hardware made by Litton and Paravant) was in public use and/or available to the public no later than March 21, 2003, and was made available by the U.S. Army. The FBCB2 system, as set forth in this chart, anticipates the asserted claims of the '838 patent at least under pre-AIA 35 U.S.C. §§ 102(a) and (g)(2) (and AIA 35 U.S.C. §§ 102(a)(1)), and/or renders the asserted claims obvious under 35 U.S.C. § 103 either alone, in combination with the general knowledge of one of ordinary skill in the art, and/or in combination with the references identified in Apple's invalidity contentions, including as set forth in this chart. On information and belief, the FBCB2 system is described at least in the following documents and other materials cited in this chart:

- *Force XXI Battle Command Brigade and Below-Blue Force Tracking (FBCB2-BFT). A Case Study in the Accelerated Acquisition of a Digital Command and Control System during Operations Enduring Freedom and Iraqi Freedom*, by James L. Conatser and Vincent E. Grizio, dated December 2005 and retrieved from <http://www.dtic.mil/dtic/tr/fulltext/u2/a443273.pdf> on November 21, 2017 ("FBCB2-1") (APL-AGIS_00012804 - APL-AGIS_00012876).
- *Blue Force Tracking The Afghanistan and Iraq Experience and Its Implications for the U.S. Army*, by Richard J. Dunn, III, stamped with a copyright dated 2003 and retrieved from <http://www.northropgrumman.com/AboutUs/AnalysisCenter/Documents/pdfs/BFT-Afghanistan-and-Iraq-Exper.pdf> on November 21, 2017 ("FBCB2-2") (APL-AGIS_00012877 - APL-AGIS_00012896).
- *FORCE XXI BATTLE COMMAND, BRIGADE AND BELOW (FBCB2)*, retrieved from <https://web.archive.org/web/20170204113146/http://www.dote.osd.mil/pub/reports/FY1999/pdf/army/99fbc2.pdf> on November 21, 2017 ("FBCB2-3") (APL-AGIS_00012800 - APL-AGIS_00012803).
- *FBCB2-BFT Family of Products*, Northrop Grumman Space & Mission Systems Corp. (2003) ("FBCB2-4") (SIEGEL000001-SIEGEL000002)
- *FBCB2 Blue Force Tracking* (Promotional Video), Northrop Grumman (2004) ("FBCB2-5") (SIEGEL000003)
- Pamela Bowers, *The TRW Tactical Systems Division Builds the Next Generation of Tactical Army Operations Systems*, CrossTalk: The Journal of Defense Software Engineering (January 2002). ("FBCB2-6") (SIEGEL000004-SIEGEL000008)

le's Invalidation Contentions Under Patent Rule 3-3
 bit D-14

- T. Trent Gegax, *Wired for Battle*, Newsweek (March 3, 2003). (“FBCB2-7”) (SIEGEL000009-SIEGEL000010)
- Vernon Loeb, *Digitized Battlefield Puts Friend and Foe in Sight*, Washington Post (March 3, 2003) (“FBCB2-8”) (SIEGEL000011-SIEGEL000013)
- Lieutenant Colonel Marc LeGare, *Battle Command and Visualization*, Military Review (September-October 2002) (“FBCB2-9”) (SIEGEL000014-SIEGEL000019)
- Neil Siegel, *Organizing Complex Projects Around Critical Skills, and the Mitigation of Risks Arising from System Dynamic Behavior*, Ph.D. Dissertation, University of Southern California (August 2011) (“FBCB2-10”) (SIEGEL000020-SIEGEL000300)
- *Personal User Data Terminal*, TRW Systems Ltd. (February 7, 2001) (“FBCB2-11”) (SIEGEL000301-SIEGEL000302)
- *Force XXI Battle Command Brigade-and-Below (FBCB2)*, TRW Systems Integration Group (1997) (“FBCB2-12”) (SIEGEL000303 - SIEGEL000308)
- *Information Dominance for Combat Power – Force XXI Battle Command Brigade and Below*, TRW Systems & Information Technology Group (2000) (“FBCB2-13”) (SIEGEL000309-SIEGEL000312)
- *The World's Only Existing Tactical Internet: The US Army's Force XXI Battle Command Brigade and Below*, Neil Siegel (Presentation at SMi Defense Conferences: Designing and Deploying Tactical Internets (May 24 1999) (“FBCB2-14”) (SIEGEL000316-SIEGEL000332)
- **U.S. Patent No. 6,212,559 (“FBCB2-15”) (SIEGEL000333-SIEGEL000358)**
- *US Army shares radios to avoid Gulf fratricide*, Kim Burger, Jane's Defence Weekly (March 12, 2003) (“FBCB2-16”) (SIEGEL000359-SIEGEL000361)
- *US Army expands battlefield digitization*, Scott Gourley, Jane's Defence Weekly (September 25, 2002) (“FBCB2-17”) (SIEGEL000362-SIEGEL000364)
- *Soldiers in Afghanistan to Receive New Blue Force Tracking System*, Emily Hsu, Inside the Army (October 28, 2002) (“FBCB2-18”) (SIEGEL000365-SIEGEL000366)
- *Technology Seeks to Erase Friendly Fire*, David McGuire, Newsbytes (March 27, 2003) (“FBCB2-19”) (SIEGEL000367-SIEGEL000368)
- **U.S. Patent No. 5,672,840 (“FBCB2-20”) (SIEGEL000369-SIEGEL000376)**
- **U.S. Patent No. 6,904,280 (“FBCB2-21”) (SIEGEL000377-SIEGEL000399)**

Apple's Invalidity Contentions Under Patent Rule 3-3
Exhibit D-14

U.S. Patent No. 7,278,023 (“FBCB2-22”) (SIEGEL000400-SIEGEL000417)

U.S. Army Brings Digital Future to Persian Gulf, Frank Tiboni, Defense News (November 11, 2002) (“FBCB2-23”) (SIEGEL000418)

Apple reserves the right to further supplement its contentions and evidence concerning the FBCB2 system as discovery proceeds, including by citation to additional materials or other evidence describing the operation of the system.

DOCKET
ALARM

Find authenticated court documents without watermarks at docketalarm.com.

le's Invalidation Contentions Under Patent Rule 3-3
 bit D-14

Limitation	Prior Art Disclosure
	<p>systems. However, it does provide a one way feed of Blue locations to the Army-level Global Command and Control System-Army (GCCS-A) through a “trusted guard,” which populates the “secret” COP and disseminates the blue picture back down through TOC systems to brigade level. The information passed over SATCOM is encrypted, however, it has not been “Type 1” communications security certified and, therefore, is not authorized to process secret information.”</p> <p><i>See, e.g.</i>, FBCB2-15 at 2:1-3:11 (“As interconnected networks become more complex, it also becomes more difficult to ensure that every network component has been correctly configured. The principal reason that manual network configuration is tolerated in large organizations is that in many cases the network configuration is relatively static, and the required changes are small and incremental. When a new employee joins the network or changes physical locations, it is a relatively simple matter to reconfigure the network to include his or her computer in the appropriate new location. Extensive corporate reorganizations are typically infrequent and there is usually adequate warning to make the necessary configuration changes. [] A more difficult problem is presented when frequent changes are needed in the network configuration. One example is a military communication network in which many of the computer stations are mobile and reconfiguration may be needed on a daily or even more frequent basis during military maneuvers. In this case, there is simply not enough time for manual reconfiguration of a large interconnected network of computers. [] Accordingly, there is a significant need for an automated process to reconfigure large computer networks, such as wireless military networks. Even in a commercial setting where there is usually enough time to reconfigure networks when changes occur, there is a need for a technique that would effect network reconfiguration more quickly and reliably than by manual means. The present invention satisfies this need and provides a number of other related advantages. ... The present invention resides in a system and a related method for automatically configuring or reconfiguring a large interconnected computer network under control of a user with appropriate system administration access to the network. Briefly, and in general terms, the method of the invention comprises the steps of planning a network configuration in simulated form through a graphical user interface; generating network programming data corresponding to a new configuration arrived at in the planning step; disseminating the network programming data over an existing communication network; conditioning computers in the network to switch to the new configuration on the occurrence of a triggering signal; and switching to the new</p>

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.