EXHIBIT C

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS

AGIS SOFTWARE DEVELOPMENT LLC, Plaintiff, v. APPLE INC., Defendant.	Civil Action No. 2:17-cv-513-JRG (LEAD CASE) Civil Action No. 2:17-cv-516-JRG

EXPERT REPORT OF NEIL SIEGEL REGARDING THE INVALIDITY OF U.S. PATENT NOS. 9,467,838; 9,749,829; 9,408,055; AND 9,445,251

via mathematical manipulation, to and from latitude and longitude) to the server, and the server broadcast that information to other FBCB2 devices. *See* SIEGEL000009-10. SIEGEL000014; SIEGEL000782. The recipient FBCB2 devices displayed the location information of the sender devices as symbols on the georeferenced maps at the appropriate latitude and longitude. *See* SIEGEL000009-10. Each FBCB2 device continuously reported new location to the server. *See* SIEGEL000009-10; SIEGEL000014. The location reporting rate was time and distance triggered, such that a device would send updated location information at a predetermined time interval, unless it moved further than a pre-specified distance before that time interval had passed. APL-AGIS_00012859. U.S. Patent No. 5,672,840, of which I am named inventor, describes the reporting filter incorporated in the FAAD C2I system based on an angular filter (e.g., reporting whenever the display was rotated more than a certain amount). *See also* SIEGEL000374 at 5:31-35. In FBCB2 (starting in 1995), that concept was extended from a filter for reporting based an angular threshold to one of a threshold based on time and motion. *See* SIEGEL000990-91. The information that passed the time-motion filter was the information that was continuously broadcast to other FBCB2 devices, and the updated information was automatically plotted on each FBCB2 device's georeferenced map. *See* SIEGEL000009-10; SIEGEL000305.

71. The servers in FBCB2 consisted of computers mounted in army vehicles. That is, individual FBCB2 units were designated to receive information from FBCB2 devices and forward it to other FBCB2 devices. Because users moved around and access to a particular server could be blocked by buildings, mountains, jamming, or other difficulties, there was not a single, static server designation in FBCB2 as there typically is in an office or consumer computer network. Instead, FBCB2 devices were programmed to collaborate and *dynamically* select one of their number to act as the server. If the unit acting as a server became unavailable for some reason—

whether because it was blocked or due to damage in the war—the remaining units would collaborate and select another of the members to take over the role of server. Thus, a given FBCB2 device could send and receive information via one or more servers during any given operation. This process for dynamically electing servers was designed and built in 1997 and 1998, and is documented in 1997 project status report (*see* SIEGEL000794-5) and 1998 design document (*see* SIEGEL001003-5). Design cases are provided for both what is termed "self-election" (where an FBCB2 computer detects that no other computer is acting as a server in an area, perhaps because this computer is the first one to start up after the arrival of a new military unit in an area) and "fractured net" (this is the use-case where server disconnects due to changes in the battlefield situation are accommodated) situations. *See* SIEGEL001003-5).

72. FBCB2-enabled devices communicated with FBCB2 servers via the internet. FBCB2 could be operated over the commercial internet, and, in fact, this was sometimes done when FBCB2 was being built and tested in the United States, and when training soldiers abroad in theaters of war. In the field, FBCB2 used a special Internet called the "Tactical Internet." *See* SIEGEL000014; SIEGEL000305. The Tactical Internet was a communication network that combined secure military communications devices (radios or satellites) with commercial TCP / IP protocols, and special adaptations to make these commercial protocols work over the radios and satellites (while preserving the ability of the network to operate regular commercial software, such as TCP / IP – based internet browsers). The Tactical Internet transmitted data via the Enhanced Position Location Reporting System (EPLRS) data radio, a data-capable version of the Single Channel Ground Air Radio System, WiFi wireless LAN (IEEE standard 802.11 and its variants), and/or L-band commercial satellites. SIEGEL000014; SIEGEL000303; SIEGEL000316; SIEGEL000361. Like devices connected to the commercial internet, devices exchanging data via

3. "participating in the group, wherein participating in the group includes sending first location information to a first server and receiving second location information from the first server, the first location information comprising a location of the first device, the second location information comprising one or more locations of one or more respective second devices included in the group;"

99. FBCB2 devices exchanged location information via a server. Each device obtained its own location from a GPS receiver attached to (or built into) the device.[7] The location information consisted of latitude and longitude coordinates determined by a GPS unit installed in the FBCB2 device. *See also* SIEGEL000009-10; SIEGEL000014; SIEGEL000782. Each device reported its latitude and longitude to the server, and the server broadcast that information to other FBCB2 devices. *See also* SIEGEL000009-10.

100. The servers in FBCB2 consisted of computers mounted in army vehicles. That is, individual FBCB2 units were designated to receive information from FBCB2 devices and forward it to other FBCB2 devices. Because users moved around and access to a particular server could be blocked by buildings, mountains, jamming, or other difficulties, there was not a single, static server designation in FBCB2 as there typically is in an office or consumer computer network. Instead, FBCB2 devices were programmed to collaborate and *dynamically* select one of their number to act as the server. If the unit acting as a server became unavailable for some reason—whether because it was blocked or due to damage in the war—the remaining units would collaborate and select another of the members to take over the role of server. This process for dynamically electing servers was designed and built in 1997 and 1998, and is documented in 1997 project status report (*see* SIEGEL000794-5) and 1998 design document (*see* SIEGEL001003-5).

[7] Location information could also be obtained by other methods, including radio triangulation of the ground-to-ground radio links or an inertial navigation system on the vehicle. The FBCB2 software automatically determined which of these was the most accurate at the moment, and used that most-accurate position as the FBCB2 position to report to the FBCB2 network.

DOCKET ALARM

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.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.