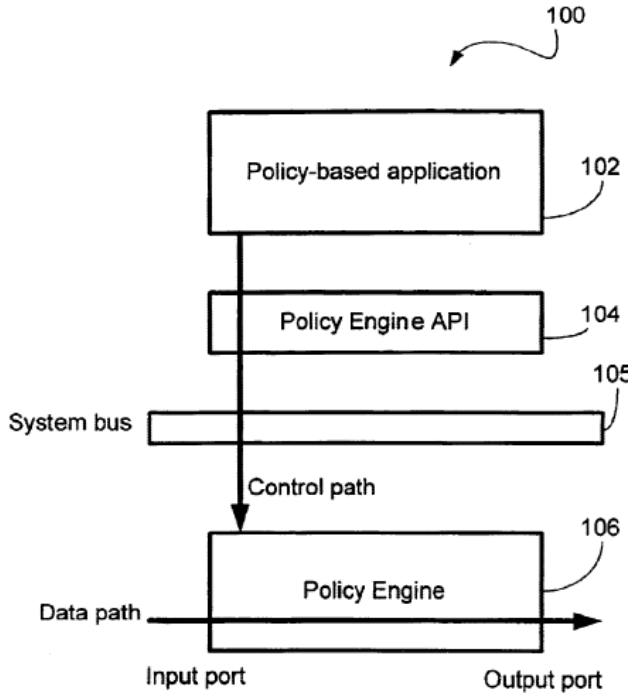
PALO ALTO'S INVALIDITY CONTENTIONS
Exhibit A13: U.S. Patent No. 6,625,150 ("Yu")

As demonstrated in the claim charts below, the Asserted Claims are invalid (a) under one or more sections of 35 U.S.C. § 102 as anticipated by Yu and (b) under 35 U.S.C. § 103(a) as obvious over Yu standing alone and as set forth herein, and/or combined with the knowledge of a person of ordinary skill in the art, admitted prior art, and/or the additional prior art references discussed in Exhibits A1-A16, and B, the contents of which are hereby incorporated by reference into this chart. Although the following charts illustrate where Yu discloses the preambles of the Asserted Claims, Palo Alto does not imply by these contentions that the preambles are claim limitations.

'099 Claim	Claim Element	U.S. Patent No. 6,625,150 ("Yu")
[1.pre]	A packet monitor for examining packets passing through a connection point on a computer network in real-time, the packets provided to the packet monitor via a packet acquisition device connected to the connection point, the packet monitor comprising:	Yu discloses a packet monitor for examining packets passing through a connection point on a computer network in real-time, the packets provided to the packet monitor via a packet acquisition device connected to the connection point. For example, Yu discloses: Abstract ("A policy engine for handling incoming data packets. The policy engine includes a stream classification module, a data packet input/output module, and a policy enforcement module. The policy enforcement module further includes a packet scheduler, an on-chip packet buffer circuitry, and a plurality of action processors. The stream classification module creates a packet service header for each data packet, wherein the packet service header indicates policies to be enforced for that data packet. The action processors enforce the policies."); 2:51-65 ("The architecture 100 includes three major components—a Policy-Based Application 102, a Policy engine API 104 ("API" stands for Application Program Interface") and a Policy engine 106. As can be seen from FIGS. 2 and 3, the policy-based application 102—such as a firewall, virtual private network (VPN), or traffic management—is typically a "legacy" software program residing on a host, equipped with its own policy database 202 and flow classifier logic 204. The policy engine API 104 serves as an interface between the policy application 102 and the policy engine 106 (via a system bus 105). The policy engine 106 is a

'099 Claim	Claim Element	U.S. Patent No. 6,625,150 ("Yu")
		purpose-built hardware (preferably running at wire speed) that operates on input network traffic and network policies and that outputs regulated traffic flows based upon the network policies."); *see also* Fig. 2, Fig. 3. 

PALO ALTO'S INVALIDITY CONTENTIONS
Exhibit A13: U.S. Patent No. 6,625,150 ("Yu")

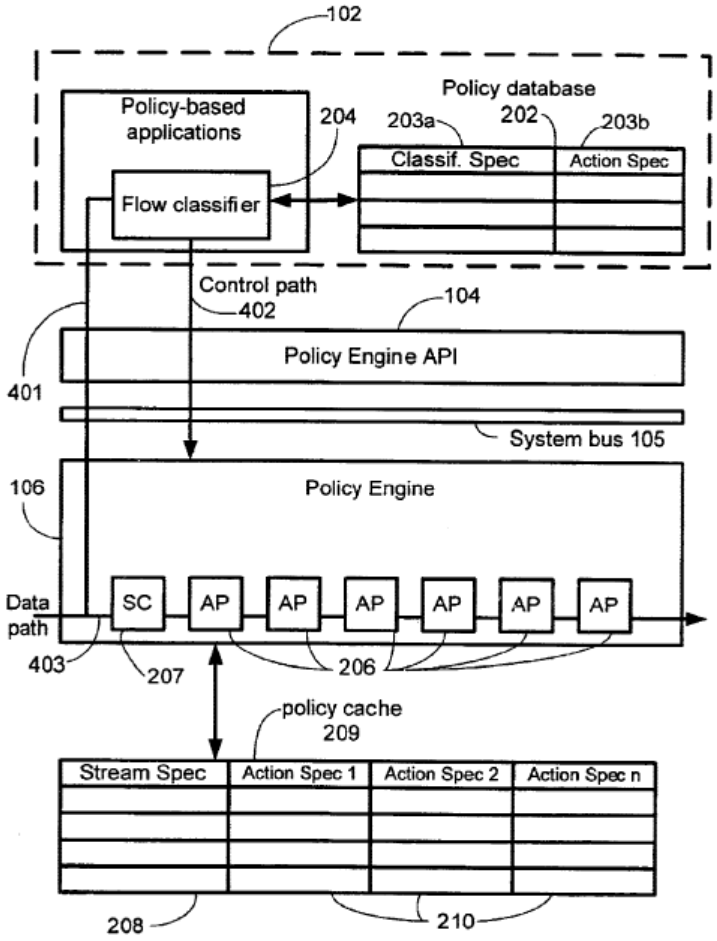
'099 Claim	Claim Element	U.S. Patent No. 6,625,150 ("Yu")
		

Fig. 3

PALO ALTO'S INVALIDITY CONTENTIONS
Exhibit A13: U.S. Patent No. 6,625,150 ("Yu")

'099 Claim	Claim Element	U.S. Patent No. 6,625,150 ("Yu")
[1.a]	(a) a packet-buffer memory configured to accept a packet from the packet acquisition device;	Yu discloses a packet-buffer memory configured to accept a packet from the packet acquisition device. For example, Yu discloses: Abstract ("A policy engine for handling incoming data packets. The policy engine includes a stream classification module, a data packet input/output module, and a policy enforcement module. The policy enforcement module further includes a packet scheduler, an on-chip packet buffer circuitry, and a plurality of action processors. The stream classification module creates a packet service header for each data packet, wherein the packet service header indicates policies to be enforced for that data packet. The action processors enforce the policies."); 6:10-15 ("The Packet Input/Output Module 402 receives packets, places the received packets in the external packet memory 450 and notifies the Stream Classification Module 404 of such packets. Upon completion of all policies enforcement, the Packet Input/Output Module 402 transmits the packet from external packet memory 450 to the network."); 6:31-58 ("The Policy Enforcement Module 406 includes a Packet Scheduler 408, On Chip packet Buffer(s) 410, and at least one Action Processor 412. The Packet Scheduler 408 copies packets from external packet memory 450 to the On Chip Packet Buffer 410. After copying the packets to the Packet Buffer 410, packets are fragmented into 64 bytes cells. An 8-bit Cell Service Header (FIG. 6) is added to the beginning of each 64-byte cell. The Cell Service Header includes a Packet Number to uniquely identify a packet in the Policy Enforcement Module pipeline and a Start bit and Stop bit to indicate the first and last cell of a packet. A Next AP field, together with the AP IDs in the Packet Service Header, indicates to the Policy Enforcement Module 406 what is the next destination Action Processor of each cell.

'099 Claim	Claim Element	U.S. Patent No. 6,625,150 ("Yu")
		It is preferable to have the On Chip Packet Buffer 410 because it allows the Action Processors 412 very low latency and high bandwidth access to the packets as compared with having to access the external Packet Memory 450. In case the next Action Processor 412 is busy for a cell, the On Chip Packet Buffer 410 serves as temporary storage for that cell. This prevents the blocking of following cells which need to go through this same Action Processor 412. Each Action Processor 412 performs a particular policy enforcement. In addition to this, it is capable of reading the required action spec based on the AP pointer on the packet Service Header (FIG. 5). Each Action Processor may also have its own input and/or output FIFO to buffer the cells."); Claim 1 ("wherein the stream classification module creates a packet service header for each packet in the external packet memory indicating, based on a policy cache, policies to be enforced on that packet;"); *see also* Fig. 4.

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.