EXHIBIT D-1
U.S. Patent App. Pub. No. 2007/0079307 ("Dhawan")

Microsoft contends that the asserted claims of the '209 Patent are invalid as obvious by U.S. Patent Application Publication No. 2007/0079307 ("Dhawan") prior art reference under various subsections of 35 U.S.C. § 102 in view of other prior art references under 35 U.S.C. § 103 as set forth in Microsoft's invalidity contentions.

As Dhawan was filed on September 30, 2005, and published by the U.S. Patent and Trademark Office by no later than April 5, 2007, Microsoft contends that it is prior art to the '209 Patent under at least pre-AIA 35 U.S.C. § 102(e).

Patent No. 8,381,209	Dhawan
Claim 1	
1[Pre] A computer implemented method of controlling network security of a virtual machine,	To the extent the preamble is limiting, Dhawan discloses a computer implemented method of controlling network security of a virtual machine. Specifically, Dhawan discloses a method for the secure transfer of data by carrier virtual machines between participating physical hosts through a virtual network (VNET) implemented on one or more internal and/or external networks. For example, Dhawan states: "A system and method is disclosed for the secure transfer of data by carrier virtual machines between participating physical hosts through a virtual network (VNET) implemented on one or more internal and/or external networks." Dhawan at Abstract. "In accordance with the present invention, a system and method is disclosed for virtual machines implemented as carriers of a payload that may include applications, data, another virtual machine etc. In various embodiments of the invention, virtual machines carrying the payload can be routed between physical hosts, based on set policies providing a secure, manageable and highly flexible environment for data and process management. Those of skill in the art will realize that many variations and implementations of such embodiments are possible." Dhawan at [0017]. "When coupled with encryption, the system and method of the invention described in more detail hereinbelow can provide a secure environment for data/application management among multiple physical hosts. Data to be transported is first encrypted and then encapsulated by a carrier virtual machine at each stage of the migration process among the physical hosts involved. To implement various embodiments of the invention requires an infrastructure, such as that provided by VMware or the Xen open source environment, to create and manage virtual machines." Dhawan at [0018].

EXHIBIT D-1
U.S. Patent App. Pub. No. 2007/0079307 ("Dhawan")

Patent No. 8,381,209	Dhawan
Claim 1	
	To the extent that it is argued that Dhawan does not disclose all or part of this limitation, it would have been at least obvious to combine it with any other reference disclosing this limitation as explained in Microsoft's Preliminary Invalidity Contention Cover Pleading.
1[a] the method comprising enforcing network security and routing at a hypervisor layer via dynamic updating of routing controls initiated by a migration of said virtual machine from a first device to a second device.	Dhawan discloses enforcing network security and routing at a hypervisor layer via dynamic updating of routing controls initiated by a migration of said virtual machine from a first device to a second device. Specifically, Dhawan teaches migration of a virtual machine from a first device to a second device; the virtual machine migration causes the routing controls to update continuously with each migration that occurs. For example, Dhawan states: "A VNET is typically established at layer 2 of the OSI network model. Through the use of layer 2 tunneling and by translating between physical and virtual network addresses, a VNET can create the illusion of a local area network, even when physical network resources are spread over a wide area. Since a VNET is established at layer 2, a virtual machine can be migrated from site to site without changing its presence, as it keeps the same media access control (MAC) and IP addresses, network routes, etc. Furthermore, since VNETs are decoupled from the underlying network topology, they are able to maintain network connectivity during virtual machine migration." Dhawan at [0014]. "In accordance with the present invention, a system and method is disclosed for virtual machines implemented as carriers of a payload that may include applications, data, another virtual machine etc. In various embodiments of the invention, virtual machines carrying the payload can be routed between physical hosts, based on set policies providing a secure, manageable and highly flexible environment for data and process management. Those of skill in the art will realize that many variations and implementations of such embodiments are possible." Dhawan at [0017]. "The carrier virtual machine is then migrated to the next participating physical host. Using the policy based Autorun Engine; necessary actions can be taken at each host. Examples may include transferring of data to the physical host or to a virtual machine in the physical host through a virtual network, to any other physical or virtual machine, a payload application gathering data or performing some maintenance on the physical or virtual machine, destroy itself if VM is on an unidentifiable host, change network interface properties like set new MAC address etc. In an embodiment of the invention, payload is transferred to a next carrier virtual machine through a virtual network implemented between

Patent No. 8,381,209	Dhawan
Claim 1	
	the originating carrier VM and a carrier VM established on the participating physical host next to initiator in the migration path." Dhawan at [0020]. "In this embodiment of the invention, carrier virtual machine 426 is migrated from participating physical host 302 using a multi-layer communications protocol stack as described in more detail herein, through network 128 to router 306. Router 306 receives IP packets through network access port '1' 308, examines the destination IP address contained in IP datagrams generated by IP layer 318, and routes IP packets through network access port '2' 310 to the designated destination IP address. In this same embodiment, participating physical host '2' 304 receives incoming IP packets through its associated multi-layer communications protocol stack to implement virtual machine 438, comprising, but not limited to virtual machine autorun scripts 428, and payload 429 that includes operating systems 430, other virtual machines 432, applications 434, and data 436. Once carrier virtual machine 426 has completed migration to participating physical host '2' 304 as virtual machine 438, carrier virtual machine 426 on participating physical host '1' 302 can be destroyed (if required by security policies)." Dhawan at [0043]. "In an embodiment of the invention, predetermined routing table 506 manages originating and terminating network addresses. In an embodiment of the invention, predetermined routing table 506 can translate between physical network addresses and virtual network addresses as typically implemented in a virtual network (VNET) whether the VNET is implemented on a Local Area Network (LAN), a Wide Area Network (WAN) such as the Internet or a corporate intranet, or a combination of public and/or private network technologies and protocols. In an embodiment of the invention, predetermined routing table 506 may also include routing, event tree, and security information regarding individual physical or virtual network hops between two endpoints." Dhawan at [0048]. "Skilled practitioners of the art will be aware that a VNET is typically established at layer 2 of the OSI network model. Through the use of layer 2 tunneling and by translating between physical and virtual network addresses, a VNET can create the illusion of a local area network, even when physical network resources are spread over a wide area. Since a VNET is established at layer 2, a virtual machine can be migrated from site to site without changing its presence, as it keeps the same media

Patent No. 8,381,209	Dhawan
Claim 1	
	access control (MAC) and IP addresses, network routes, etc. Furthermore, since VNETs are decoupled from the underlying network topology, they are able to maintain network connectivity in its original form during/after virtual machine migration." Dhawan at [0072]. To the extent Dhawan does not disclose dynamically updating the routing control, it would have at least been obvious to combine Dhawan with prior art disclosing this as demonstrated in Microsoft's Invalidity Contentions Cover Pleading.

Patent No. 8,381,209	Dhawan
Claim 2	
2[a] The method according to claim 1, further comprising: routing traffic for the virtual machine to the second device at the hypervisor layer; and	Dhawan discloses routing traffic for the virtual machine to the second device at the hypervisor layer. Specifically, Dhawan discloses a hypervisor that sets the contents of an IP datagram, including the destination IP addresses. For example, Dhawan states: "In an embodiment of the invention, a user specifies which payload should be secured and needs to be sent to particular hosts. A special carrier virtual machine (VM) is created that can transfer the payload to its predetermined destination host(s). VM migration and/or routing tables are built in the carrier VM, which determine which hosts will be participating. A connection is made to the target host(s) to accept the request for transferring the virtual machine. The specified payload is (or can be encrypted and then) encapsulated in a carrier VM. Typically, a "time-to-live" attribute is also set for VM. If the VM fails to migrate to its next hop/does not completed intended task at the host in the specified time, it can notify the sender then destroy itself and hence the payload it contains, send a request to the originating host for a time-to-live extension if network is congested, request a reroute due to high traffic on a predetermined route or access policies etc, or other predetermined actions." Dhanwan at [0019]. "In the present invention, a virtual machine monitor 116 sets the contents of IP datagram header fields, including but not limited to, service type 208, time to live 218 and destination IP address 226. In an implementation of one embodiment of the invention, a participating physical host can receive a carrier virtual machine and set the destination IP address 226 to forward the carrier virtual machine to the

Patent No. 8,381,209	Dhawan
Claim 2	
	destination IP address of the next for the next participating physical host. This process can be repeated to implement a flexible, yet secure, carrier virtual machine routing path over one or more networks." Dhawan at [0039]. To the extent that it is argued that Dhawan does not disclose all or part of this limitation, it would have been at least obvious to combine it with any other reference disclosing this limitation as explained in Microsoft's Preliminary Invalidity Contention Cover Pleading.
2[b] setting firewalls to permit a network traffic for the virtual machine to go to the second device at the hypervisor layer.	Dhawan discloses setting firewalls to permit a network traffic for the virtual machine to go to the second device at the hypervisor layer. Specifically, Dhawan discloses setting firewalls to protect virtual networks from exposure of sensitive data and the identity of systems involved. For example, Dhawan states: "One of the challenges in secure computing and network environments is hiding the identities of the originator and intended recipient of highly sensitive data. Hackers continue to use creative approaches to monitor network activity, especially in identifying high profile candidate IP/MAC addresses, and high value data conduits or paths within a network. Various techniques can be used against these malicious monitors to protect against exposure of sensitive data and the identity of systems involved, including firewalls, data encryption, traffic camouflaging, etc. However, these methods are not fool proof and they each have characteristics that can result in attendant issues." Dhawan at [0006]. "In an embodiment of the invention, virtual machine (VM) packet management 504 comprises parameters that may include, but are not limited to, time-to-live (TTL), security mechanisms such as access control lists (ACLs), usage policies, directory roles, etc. for carrier virtual machine 120, and by extension, application 122 and/or secure data 124, individually or in combination. For example, VM packet management 504 may control the flexibility of hardware and/or software access for VM network endpoints and/or intermediate routing hops. As another example, the VM packet management 504 may instantiate quarantining of all VM packets, a group of packets, a single VM, subpackets within a VM between network endpoints, or at a predetermined intermediary network point. VM packet management 504 may also manage access to carrier virtual machine payloads by security groups, individual access, subdivided individual access, and MIME-like subdivision of a VM-

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.