The Columbia

SCIENCE AND TECHNOLOGY LAW REVIEW

www.stlr.org

AN ANTITRUST TYING ANALYSIS OF MICROSOFT'S SECURITY SOFTWARE PRODUCTS

Heather Schneider[*]

This article discusses the possible legal ramifications of Microsoft's recent entry into the market for security software, such as personal firewall, anti-virus, and anti-spyware software. Microsoft has encountered antitrust problems in the past by bundling software with the Windows operating system, and some commentators have suggested that Microsoft's next antitrust battle will be over security software. The purpose of this article is to determine whether Microsoft's new security offerings could constitute illegal tying arrangements. The article provides a technical background, including a description of operating systems and security software in general, an overview of Microsoft's current and proposed security offerings, and reasons why security software is needed. It then discusses the hypothetical outcome of a tying claim against Microsoft under Section 1 of the Sherman Act by analyzing Microsoft's product offerings under the traditional *per se* tying rule and under the rule of reason. It concludes by presenting several possible remedies if a tying violation were to be found.

INTRODUCTION

Microsoft[1] made waves in the software industry in late 2004 and early 2005 by announcing its entry into the security software market for personal computers. In December 2004, Microsoft announced its acquisition of anti-spyware maker Giant Company Software.[2] Then in January 2005, Microsoft released beta versions of two free tools for the removal of spyware and viruses,[3] causing an immediate drop in the stock price of security companies

[*] Columbia Law School, J.D. Candidate 2006. Executive Editor, Columbia Science & Technology Law Review, Vol. VII. The author would like to thank Ryan Schneider, Professor Robert Pitofsky, and William H. Rooney for their comments and suggestions.

[1] The names of companies and products mentioned herein may be the trademarks of their respective owners.

[2] Neil J. Rubenking, *Microsoft Acquires Giant, Plans Antispyware Release*, PC Magazine.com, Dec. 16, 2004, http://www.pcmag.com/article2/0,1759,1743165,00.asp.

[3] Spyware is "[a]ny software that covertly gathers user information through the user's Internet connection

Symantec and McAfee.[4] In February 2005, Microsoft announced plans to buy anti-virus maker Sybari Software.[5] Even before this series of events, Microsoft had delivered new security features to home users in August 2004 as part of its latest update for the Windows operating system, known as a "service pack."[6] Windows XP Service Pack 2 (SP2) included a centralized security interface and updated personal firewall software.[7]

Initially, many competitors tried to downplay Microsoft as a potential threat in the security market, saying it would take years for Microsoft to become truly competitive with its newly acquired technologies.[8] However, an analyst from Gartner, a leading information technology research firm, predicted that Microsoft's entry into the security market could threaten a wide range of security companies as Microsoft expands beyond anti-spyware.[9] This threat became more of a reality in May 2005, when Microsoft announced its development of a new all-in-one security software product called Windows OneCare.[10]

The author's fear is that Microsoft's entry into this market will drive away many competitors, chilling innovation in the security software market and resulting in less security for end users. In an age when hundreds of computer viruses are on the loose at any given time and virus outbreaks generate more corporate losses than certain types of theft,[11] it is especially

without his or her knowledge, usually for advertising purposes." Definition of Spyware, http://www.webopedia.com/TERM/S/spyware.html (last visited Nov. 16, 2005). A virus is "[a] computer program that replicates itself and transfers itself to another computing system." Dictionary, AccessScience@McGraw-Hill, http://www.accessscience.com (last visited Nov. 16, 2005).

[4] Jaikumar Vijayan, *Microsoft Releases Antispyware, Malware-removal Tools*, Computerworld.com, Jan. 6, 2005, http://www.computerworld.com/securitytopics/security/story/0,10801,98783,00.html; Paul Roberts, *Microsoft Move Sends Shivers Through Antivirus Market*, Computerworld.com, Jan. 7, 2005, http://www.computerworld.com/softwaretopics/os/windows/story/0,10801,98802,00.html.

[5] Dawn Kawamoto, *Microsoft to Buy Antivirus Software Firm*, CNET News.com, Feb. 8, 2005, http://news.com.com/Microsoft+to+buy+antivirus+software+firm/2100-7350_3-5567529.html?tag=st.rn.

[6] *See generally* Microsoft Service Packs, http://support.microsoft.com/sp (last visited Nov. 16, 2005) ("Service packs are the means by which product updates are distributed. Service packs may contain updates for system reliability, program compatibility, security, and more.").

[7] Robert Lemos & Dawn Kawamoto, *Windows Anti-spyware to Come Free of Charge*, CNET News.com, Feb. 15, 2005, http://news.com.com/Windows+anti-spyware+to+come+free+of+charge/2100-7355_3-5577202.html.

[8] Matt Hines, *Long Fuse for Microsoft's Security Challenge*, CNET News.com, Feb. 16, 2005, http://news.com.com/Long+fuse+for+Microsofts+security+challenge/2100-7355_3-5579418.html.

[9] *Id.*; *see generally* About Gartner, http://www.gartner.com/it/about_gartner.jsp (last visited Nov. 16, 2005) (Gartner, Inc. claims to be the "world's leading provider of research and analysis about the global information technology industry.").

[10] Press Release, Microsoft Corp., Microsoft to Deliver Automated, All-in-One PC Health Service for Consumers (May 13, 2005), http://www.microsoft.com/presspass/press/2005/may05/05-13WindowsOneCarePR.mspx.

[11] Deborah Asbrand, *Is Microsoft's AntiVirus Strategy Secure?*, TechnologyReview.com, Jan. 20, 2005, http://www.technologyreview.com/articles/05/01/wo/wo_asbrand012005.asp ("In the Computer Security Institute's 2004 CSI/FBI Computer Crime and Security Survey, virus outbreaks emerged for the first time as the incident type generating the largest culprit for corporate losses, edging out theft of proprietary information, which had been the

important to have a variety of vibrant and innovative competitors searching for solutions to security problems.

The purpose of this paper is to analyze whether Microsoft's new security products could constitute illegal tie-in sales. Microsoft has encountered antitrust problems in the past due to its bundling of software with the operating system. In a suit brought by the United States government, a district court held that Microsoft's bundling of the Internet Explorer web browser constituted a *per se* violation of antitrust laws.[12] The court of appeals rejected this analysis and remanded for the district court to apply the rule of reason.[13] The tying claim was dropped by the government, so it is not clear what the district court's ruling would have been on remand.[14] In a similar case in Europe, the European Commission found that Microsoft's bundling of the Windows Media Player was an illegal tie, and forced Microsoft to release a version of the operating system without the software.[15] In the United States, Microsoft recently paid RealNetworks over $400 million to settle its antitrust claims involving the bundling of Windows Media Player.[16] Commentators have suggested that Microsoft's next antitrust battle will be over security software.[17] The European Commission already appears to be investigating Microsoft's security products and was recently given some information by security company Symantec.[18]

Part I of this note provides a technical background, including a description of operating systems and security software in general, an overview of Microsoft's current and proposed security offerings, and reasons why security software is needed. Part II then discusses the outcome of a potential tying claim against Microsoft under Section 1 of the Sherman Act. It analyzes Microsoft's products under the traditional *per se* tying rule and under the rule of reason. Part III discusses possible remedies if a tying violation were to be found.

I. TECHNICAL OVERVIEW

This section provides an overview of the technologies involved. It describes the software products that are discussed throughout the rest of this Note and explains why users who run Microsoft Windows need security software.

most expensive category of loss for five years.").

[12] *United States v. Microsoft Corp.*, 87 F. Supp. 2d 30, 47-51 (D.D.C 2000) , *aff'd in part, rev'd in part, and remanded*, 253 F.3d 34 (D.C. Cir. 2001) (en banc).

[13] *United States v. Microsoft Corp.*, 253 F.3d 34, 84-97 (D.C. Cir. 2001) (en banc).

[14] Thor Olavsrud, *DOJ Calls Off Microsoft Break-Up Effort*, Internetnews.com, Sept. 6, 2001, http://www.internetnews.com/bus-news/article.php/879531.

[15] Jeremy Kirk, *Security: Microsoft's Next Antitrust Battle?*, PCWorld.com, Oct. 13, 2005, http://www.pcworld.com/resource/article/0,aid,123008,pg,1,RSS,RSS,00.asp.

[16] Ina Fried, *Real, Microsoft Reach Truce*, CNET News.com, Oct. 11, 2005, http://news.com.com/Real%2C+Microsoft+reach+truce/2100-1030_3-5893069.html.

[17] Kirk, *supra* note 15.

[18] *Id.*

A. *The Operating System*

The operating system is the "command center"[19] or "brain"[20] of a computer. It is "responsible for managing and coordinating activities and sharing the resources of the computer."[21] It manages the computer's hardware and provides a set of application programming interfaces (APIs) that allow other programs to communicate with input/output devices such as printers and keyboards.[22] The operating system manages memory, so that several applications can run on a computer at the same time.[23] It also manages the file system so that users and applications can save data in files on the computer's hard disk.[24] It provides security to prevent unauthorized access to the computer, for example by asking users for a password to log in.[25]

The operating system that Microsoft currently offers for personal computers (PCs) is called Windows XP.[26] The next version of Windows (formerly code-named Longhorn) has been named Windows Vista and is currently in beta testing.[27] Microsoft releases a service pack to update the operating system about once a year; the last update was called Windows XP SP2.[28] According to Microsoft, SP2 is "all about security" and provides protection from viruses and malicious intruders by including the Windows Firewall, a Pop-up Blocker for Internet Explorer, and the new Windows Security Center.[29]

Microsoft delivers its Service Packs through the Windows Update utility. According to Microsoft, "Windows Update is the online extension of Windows that helps you to keep your

[19] *In re Cusumano v. Microsoft Corp.*, 162 F.3d 708, 710 (1st Cir. 1998) (citing *United States v. Microsoft Corp.*, No. 98-2133, 1998-2 Trade Cas. (CCH) ¶72,261, at 1 (D.D.C. Dec. 15, 1998)).

[20] *Hubco Data Prods. Corp. v. Mgmt. Assistance, Inc.*, 219 U.S.P.Q. (BNA) 450, 451 (D. Idaho 1983).

[21] Curt Schimmel, *Operating System*, AccessScience@McGraw-Hill, http://www.accessscience.com (DOI 10.1036/1097-8542.470405) (last visited Oct. 30, 2005).

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *See* Microsoft Windows XP Home Page, http://www.microsoft.com/windowsxp/default.mspx (last visited Nov. 8, 2005).

[27] *See generally* Microsoft Windows Vista, http://www.microsoft.com/windowsvista/default.mspx (last visited Nov. 8, 2005).

[28] *See* Microsoft Windows XP Service Pack 2, http://www.microsoft.com/windowsxp/sp2/default.mspx (last visited Nov. 8, 2005).

[29] *Id.*

computer up-to-date."[30] Users can visit the web site to look for updates or turn on the "Automatic Update" feature in Windows which will automatically find and download high-priority updates.[31] There are currently "more than 112 million Windows XP PCs configured to receive updates automatically."[32] This should make Windows Update a very effective distribution tool.

B. *Personal Firewall Software*

Firewalls are "hardware and software programs that protect the resources of a private network from users in other networks, controlling all traffic according to a predefined access policy."[33] Typically, corporations use firewalls to secure their intranets (their internal company networks) from unauthorized access by users on the Internet.[34] A firewall resides at a network's connection point to the Internet and analyzes passing data streams, either allowing or forbidding data to pass based on a set of security policies or rules.[35] Companies use firewalls to keep malicious intruders out of their internal networks and to monitor or prevent employee access to the Internet.[36]

This Note is concerned with the market for what is known as *personal firewall* software. This software runs on an individual's PC to keep out malicious intruders. Like corporate firewalls, personal firewalls may also monitor inbound and outbound network traffic and protect a computer's network connection points from infiltration.[37] The importance of personal firewalls has increased as more and more home users have high-speed permanent Internet connections such as DSL and cable modems.[38]

[30] About Microsoft Windows Update, http://v4.windowsupdate.microsoft.com/en/about.asp (last visited Nov. 7, 2005).

[31] Stay Up to Date Automatically (Oct. 12, 2004), http://www.microsoft.com/windowsxp/using/setup/getstarted/autoupdates.mspx.

[32] *See* Paul Roberts, *Microsoft Sends Shivers Through Antivirus Market*, PCWorld.com, Jan. 6, 2005, http://www.pcworld.com/news/article/0,aid,119197,00.asp.

[33] Encyclopedia of Science and Technology Online, AccessScience@McGraw-Hill, http://www.accessscience.com (search for "firewall"; then select "dictionary" tab) (last visited Nov. 1, 2005).

[34] Definition of Firewall, http://www.webopedia.com/TERM/f/firewall.html (last visited Nov. 8, 2005).

[35] *Checkpoint Sys. v. Check Point Software Techs., Inc.*, 104 F. Supp. 2d 427, 440 (D.N.J. 2000), *aff'd*, 269 F.3d 270 (3d Cir. 2001).

[36] For example, a company can search through firewall log files to locate employees who are using their work computers to look at pornography. *See, e.g.*, *United States v. Simons*, 29 F. Supp. 2d 324, 326 (E.D. Va. 1998) (where a manager conducted a search for the word "sex" in the firewall logs to determine that an employee had been looking at x-rated web sites at work), *aff'd*, 206 F.3d 392 (4th Cir. 2000) .

[37] Sheryl Canter, *You Need a (Properly Configured) Firewall*, PC Magazine.com, Oct. 5, 2004, http://www.pcmag.com/article2/0,1759,1647698,00.asp.

[38] Jeff Tyson*, How Firewalls Work*, HowStuffWorks.com, http://computer.howstuffworks.com/firewall.htm (last visited Nov. 8, 2005).

Microsoft offered an Internet Connection Firewall in the original version of Windows XP.[39] This firewall, which has been described as "barely usable,"[40] did not contain many of the features that come with most commercial firewalls. Microsoft included a more sophisticated firewall with the release of Windows XP SP2 in 2004.[41] The new version helps block viruses, asks permission to block or unblock certain network requests, and provides a log of security events.[42] Microsoft's firewall still lacks outbound filtering, which helps prevent an infected computer from spreading viruses to other computers on the network.[43] Even the lead product manager for Windows said that the firewall is "still very rudimentary."[44]

C. *Anti-Virus Software*

One security product that most home users are likely familiar with is anti-virus software. A virus is "[a] computer program that replicates itself and transfers itself to another computing system."[45] In December 2004, 390 different computer viruses were traveling the Internet.[46] Some viruses install hidden programs (called "bots") that run on an infected computer and listen for commands to download or execute other programs from a server on the Internet.[47] These programs are often used to perform denial of service attacks against web sites, in which a large number of computers disable a web site by accessing it at the same time.[48] If a user's computer is running this type of hidden program, the user may actually contribute to one of these attacks without even knowing it.[49] A worm is another type of virus that replicates itself without the

[39] *See* Description of the Windows XP Internet Connection Firewall, http://support.microsoft.com/default.aspx?scid=kb;en-us;320855 (last visited Nov. 8, 2005).

[40] David Berlind, *Why Your Personal Firewall Could be Obsolete*, ZDNet, Apr. 27, 2004, http://techupdate.zdnet.com/techupdate/stories/main/personal_firewall_obsolete.html.

[41] *See* Understanding Windows Firewall, http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx (last visited Nov. 8, 2005).

[42] *Id.*

[43] Berlind, *supra* note 40.

[44] *Id.*

[45] Dictionary, AccessScience@McGraw-Hill, *supra* note 3.

[46] Asbrand, *supra* note 11.

[47] *See, e.g.,* McAfee Profile of Mydoom Virus, http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=132094 (last visited Nov. 8, 2005).

[48] Chris Morganti, *Denial of Service FAQ Basic*, SecurityDocs.com, Dec. 16, 2004, http://www.securitydocs.com/library/2774.

[49] In 2001 there were 4,000 denial of service attacks a week, including one attack that brought down several Microsoft web sites for about two hours. *See* Robert Lemos, *Study: Sites Attacked 4,000 Times a Week*, CNET News.com, May 22, 2001, http://news.com.com/2100-1001-258093.html; Robert Lemos, *Attack Knocks Out*

user's awareness, for example by sending itself to all the addresses in a user's email address book.[50] Another type of malicious software program is the Trojan horse, which tricks users into opening it because it is disguised itself as legitimate software.[51]

Microsoft first entered the anti-virus market with its purchase of a small Romanian company called GeCad in 2003.[52] Then in early 2005 it announced plans to acquire a NY-based company called Sybari Software, which provides server-level anti-virus protection for corporate networks.[53] As of October 2005, Microsoft had not yet commercially released a full-featured anti-virus software package. However, it has released a free malicious software ("malware") removal tool which can detect and remove several well-known viruses.[54] Users can run the software by visiting the Microsoft web site or by running the Windows Update utility.[55]

Competing security companies, like industry leader Symantec, are currently gearing up for a major battle with Microsoft when it releases its full anti-virus software.[56] Symantec currently makes 40% of its $2.6 billion in annual revenues from consumer anti-virus software.[57] Although Symantec's CEO says he's eager to compete with Microsoft, others feel differently:

> Make no mistake, though: Microsoft's incursion is a serious threat. It will be able to use its Windows monopoly to get its antivirus software loaded onto nearly every consumer PC. Microsoft hasn't revealed its pricing plans, but if it undercuts Symantec's $24.95-per-year subscription price, it will likely gain substantial market share. And if it gives away the software -- though, that's unlikely because of antitrust issues -- it could quickly erode the market for Symantec and others.[58]

Microsoft Web Sites, CNET News.com, Jan. 25, 2001, http://news.com.com/2100-1001-251573.html.

[50] Vangie 'Aurora' Beal, *The Difference Between a Virus, Worm, and Trojan Horse?*, http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp (last updated Oct. 29, 2004).

[51] *Id.*

[52] *See* Robert Lemos, *Microsoft Moves into Antivirus Realm*, CNET News.com, June 10, 2003, http://news.com.com/Microsoft+moves+into+antivirus+realm/2100-1002_3-1015237.html.

[53] *See* Kawamoto, *supra* note 5.

[54] Microsoft Malicious Software Removal Tool, http://www.microsoft.com/security/malwareremove/default.mspx (last visited Oct. 27, 2005).

[55] *Id.*

[56] Sarah Lacy & Steve Hamm, *Symantec's Thompson: "I Can't Wait To Compete . . ."*, Bus. Wk., Mar. 21, 2005, *available at* http://yahoo.businessweek.com/magazine/content/05_12/b3925093_mz063.htm.

[57] *Id.*

[58] *Id.*

D. *Anti-Spyware Software*

Another common security problem is the installation of spyware on home computers. Spyware is "[a]ny software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes."[59] Many people install spyware without realizing it when they install certain file-sharing software.[60] Spyware surreptitiously monitors a user's Internet activity and then transmits information (such as email addresses, passwords, and credit card numbers) to someone else.[61] The anti-spyware market is expected to boom in 2005, with 65% of businesses planning to buy programs to prevent malicious software.[62] The current market leaders are McAfee and LavaSoft, whose products were used by 42 and 36 percent of users surveyed.[63]

Microsoft entered the anti-spyware market after it finalized its purchase of Giant Software in February 2005.[64] It released a beta version in January, and announced in February that the final version would be available for free.[65] The beta can be downloaded directly from the Microsoft web site.[66] Virus writers quickly targeted Microsoft's new anti-spyware product by creating a malware program that could disable it.[67]

E. *Combination Software*

Some software might combine firewall, anti-virus, and anti-spyware functions. For example, Microsoft Windows XP SP2 provides a free Security Center which lets users check the status of various security settings.[68] This utility determines whether the computer has a firewall and anti-virus program installed (even if from another vendor) and whether Windows Update is set to download and install updates automatically. It then notifies the user if these security

[59] Definition of Spyware, *supra* note 3.

[60] *Id.*

[61] *Id.*

[62] CNET News.com Staff, *Study: Anti-spyware Market to Boom in 2005*, CNET News.com, Feb. 11, 2005, http://news.com.com/Study+Anti-spyware+market+to+boom+in+2005/2100-7350_3-5572950.html.

[63] *Id.*

[64] *See* Lemos & Kawamoto, *supra* note 7.

[65] *See id.*

[66] *See* Microsoft Windows AntiSpyware (Beta), http://www.microsoft.com/athome/security/spyware/software/default.mspx/ (last visited Nov. 8, 2005).

[67] Dan Ilett, *Trojan Attacks Microsoft's Anti-Spyware*, CNET News.com, Feb. 9, 2005, http://news.com.com/Trojan+attacks+Microsofts+anti-spyware/2100-7349_3-5569429.html.

[68] Manage Your Computer's Security Settings in One Place (Aug. 4, 2004), http://www.microsoft.com/windowsxp/using/security/internet/sp2_wscintro.mspx.

features are absent or nonfunctioning. This product allows a user to see whether or not the computer is running a firewall and anti-virus software, but it does not actually provide these services.

Microsoft is also going to offer more advanced combination products. Microsoft has announced its intentions to sell a complete all-in-one security product called Windows OneCare.[69] Unlike the Security Center, this product actually performs anti-virus, firewall, anti-spyware, and other security tasks. Microsoft is also developing a different product for business users, known as Microsoft Client Protection. [70] The announcement of these products is a little confusing, since Windows Vista will supposedly include some of these features, such as a firewall and malware removal tool.[71] In addition, Microsoft has announced that it will bundle anti-spyware software with Windows Vista.[72] Suffice it to say that as of October 2005, it is unclear whether Microsoft's future security offerings will be bundled with the operating system or will consist of separate products, and whether those separate products will be free or fee-based.

F. *Why Security Software Is Needed*

The Internet is a dangerous place for home computers. In the fall of 2004, America Online and the National Cyber Security Alliance conducted a study of 329 homes and found that 80% of the computers were infected with spyware (which 90% of the users were unaware of) and 1 in 5 had an active virus.[73] A more extensive study by the Honeynet Project found that *over one million* computers on the Internet were running unknown bot programs, which can be used to perform denial of service attacks, send spam emails, or perform mass identity theft.[74] For example, a group of Dutch criminals recently used a Trojan horse to commandeer 1.5 million computers to take part in identity theft and blackmail schemes.[75] According to the Honeynet study, "[m]any well-known vulnerabilities in the Windows operating system were exploited by 'bot net controllers to find and take over target machines" especially home computers that were

[69] *See* Press Release, *supra* note 10.

[70] Joris Evers, *Microsoft Set to Test Security Software*, CNET News.com, Oct. 6, 2005, http://news.com.com/2100-1009_3-5889842.html.

[71] *See* Microsoft Windows Vista Security, http://www.microsoft.com/windowsvista/security.mspx (last visited Nov. 8, 2005).

[72] CBR Staff Writer, *Microsoft to Bundle Anti-Spyware in Windows*, Computer Business Review Online, Oct. 18, 2005, http://www.cbronline.com/article_feature.asp?guid=3BF1E8F2-88CC-4F49-B3AB-9A4D3FAAED35.

[73] Robert Lemos, *Plague Carriers: Most Users Unaware of PC Infections*, CNET News.com, Oct. 25, 2004, http://news.com.com/Plague+carriers%3A+Most+users+unaware+of+PC+infections/2100-1029_3-5423306.html.

[74] BBC News, *Have Hackers Recruited Your PC?*, Mar. 17, 2005, http://news.bbc.co.uk/1/hi/technology/4354109.stm. For more details on the study, *see* About the Honeynet Project, http://project.honeynet.org/misc/project.html (last visited Nov. 8, 2005)

[75] Joris Evers, *Adware Maker: We were Victims of Cybergang*, CNET News.com, Nov. 3, 2005, http://news.com.com/Adware+maker+We+were+victims+of+cybergang/2100-7349_3-5930099.html.

continuously connected to the Internet via broadband connections.[76] This study and others have found that an unprotected computer can only remain on the Internet from a few seconds to twenty minutes before being compromised.[77]

There is much debate over why home computers running the Windows operating system have security problems. Some argue that Windows has basic design flaws that increase its vulnerability, while others say that Windows is no less secure than any other operating system — it is just targeted by malicious software writers because it is so popular .[78]

It is well known that releases of Windows often contain security holes that are exploited by malware writers and then patched by Microsoft. This is common knowledge because Microsoft issues security bulletins every time a new security update becomes available.[79] For example, in February 2005 Microsoft issued bulletins for twelve Windows security issues, including one vulnerability that could allow users' information to be disclosed and several vulnerabilities that could allow remote code execution.[80]

Many of Microsoft's critics argue that these problems are caused by design flaws with Windows. One complaint is that Windows was "designed to be a single-user, stand-alone PC operating system."[81] Because of this, Microsoft made certain Windows technologies "extremely powerful and without any real security."[82] Then Microsoft designed its internet products (such as Internet Explorer) to depend on these underlying technologies, which cause security issues in today's networked world.[83]

Another common security complaint relates to the Windows permission model. Although network administrators may enforce strict user privileges for networks, servers, and

[76] BBC News, *supra* note 74.

[77] *Id.* ("The longest time a Honeynet machine survived without being found by an automatic attack tool was only a few minutes. The shortest compromise time was only a few seconds."). *See also*, Kevin Mitnick, *Automated "Bots" Overtake PCs Without Firewalls Within 4 Minutes*, Avantgarde, Nov. 30, 2004, http://www.avantgarde.com/ttln113004.html (finding that home computers without firewalls were overtaken by bots within four minutes); Matt Loney & Robert Lemos, *Study: Unpatched PCs Compromised in 20 Minutes*, CNET News.com, Aug. 17, 2004, http://news.com.com/Study:+Unpatched+PCs+compromised+in+20+minutes/2100-7349_3-5313402.html (discussing a study by the Internet Storm Center which found a 20-minute "survival time" before unprotected PCs were compromised).

[78] Nicholas Petreley, *Security Report: Windows vs Linux*, The Register, Oct. 22, 2004, http://www.theregister.co.uk/security/security_report_windows_vs_linux/.

[79] Microsoft Security Updates, http://www.microsoft.com/security/bulletins/default.mspx (last updated Oct. 11, 2005). Security alerts are also provided by the United States Computer Emergency Readiness Team (US-CERT), a division of the Department of Homeland Security, at http://www.us-cert.gov/.

[80] Microsoft Security Bulletin Summary for February, 2005, Feb. 8, 2005, http://www.microsoft.com/technet/security/bulletin/ms05-feb.mspx.

[81] Steven J. Vaughan-Nichols, *You Can Run Firefox, But You Can't Take the IE Out of Windows*, eWeek.com, Mar. 15, 2005, http://www.eweek.com/article2/0,1759,1776387,00.asp.

[82] *Id.*

[83] *Id.*

other resources, individuals users often need to log on to their Windows systems as administrators in order to get programs to run properly.[84] This is because many Windows programs save their information in locations that only administrative users can access.[85] Experts say that logging on as an administrator causes security problems because virus writers "take advantage of those elevated privileges to install malicious programs and change the configuration of Windows to keep their creations from being detected, shut down, or removed."[86]

Many people argue that all operating systems have some design flaws and that Microsoft Windows is largely targeted by malicious intruders because it is so popular. For example, security company Symantec has pointed out that the Macintosh operating system also has vulnerabilities, and is experiencing more attacks as its popularity increases. [87] The ubiquitous use of Windows is surely a draw for computer criminals —this is the dark side of having a product with network effects. Generally, a user of a network effect product, such as a telephone, derives *more* benefit from the product as more people use it.[88] This is one reason the D.C. Circuit Court of Appeals found such a high barrier to entry in the operating system market.

> That barrier -- the "applications barrier to entry" -- stems from two characteristics of the software market: (1) most consumers prefer operating systems for which a large number of applications have already been written; and (2) most developers prefer to write for operating systems that already have a substantial consumer base. This "chicken-and-egg" situation ensures that applications will continue to be written for the already dominant Windows, which in turn ensures that consumers will continue to prefer it over other operating systems.[89]

However, the flip side may also be true. As more people use Windows they may actually be *less* secure since more malicious intruders may target it. People may write malicious software for Windows for the same reason legitimate application developers do – because it is so popular. Today there are 600 million PCs running Windows, and Microsoft has claimed there will be *1 billion* by 2010.[90] The Honeynet Project study has shown that criminals can target Windows to create armies of computers that can be used to send spam, attack web sites, or engage in mass

[84] Paul Roberts, *Fewer Permissions Are Key to Longhorn Security*, PCWorld.com, Apr. 7, 2005, http://www.pcworld.com/resource/article/0,aid,120314,pg,1,RSS,RSS,00.asp.

[85] *Id.*

[86] *Id.* Microsoft has apparently addressed this problem in Windows Vista. *See* Microsoft Windows Vista Security, *supra* note 71.

[87] Munir Kotadia, *Mac OS X Faces Hacker Threats: Symantec*, ZDNet Australia, Mar. 21, 2005, http://www.zdnet.com.au/news/security/0,2000061744,39185387,00.htm.

[88] *See United States v. Microsoft Corp.*, 253 F.3d 34, 49 (D.C. Cir. 2001) (en banc).

[89] *Id.* at 55 (citations omitted).

[90] Mary Jo Foley, *Microsoft: Expect 1 Billion-Plus Windows PCs by 2010*, Microsoft Watch, July 12, 2004, http://www.microsoft-watch.com/article2/0,1995,1622658,00.asp.

identity theft.[91] If a person wants to write malware to steal people's information or hijack their computers, it only makes sense to target Windows, since the pool of potential victims is so large.

II. ANALYSIS OF A TYING CLAIM

This section discusses whether or not Microsoft's inclusion of security software with Windows may constitute a tying arrangement that violates Section 1 of the Sherman Act. It first discusses the basic background of tying doctrine and then analyzes Microsoft's security offerings under the *per se* rule and the rule of reason.

A. *Basic Tying Doctrine*

Section 1 of the Sherman Act states: "Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is declared to be illegal."[92] Typical violations of Section 1 include horizontal agreements between competitors to fix prices,[93] divide territories,[94] or boycott a competitor.[95] They may also include vertical agreements between suppliers, distributors, or retailers to conduct similar activities, although these agreements are usually treated less strictly.[96]

Traditionally in antitrust law some activities, "because of their pernicious effect on competition and lack of any redeeming virtue," are treated as *per se* violations of the Act "without elaborate inquiry as to the precise harm they caused or the business excuse for their use."[97] Other activities are analyzed under the *rule of reason*, where "[t]he true test of legality is whether the restraint imposed is such as merely regulates and perhaps thereby promotes competition or whether it is such as may suppress or even destroy competition."[98] The U.S. Supreme Court generally only adopts a *per se* rule after "considerable experience with certain business relationships" and is hesitant to apply a *per se* rule of illegality to practices they have never before examined.[99]

[91] BBC News, *supra* note 74.

[92] 15 U.S.C. §1 (2000).

[93] *United States v. Socony-Vaccum Oil Co.*, 310 U.S. 150, 218 (1940).

[94] *United States v. Topco Assoc., Inc.*, 405 U.S. 596, 608 (1972).

[95] *Nw. Wholesale Stationers, Inc. V. Pac. Stationery & Printing Co.*, 472 U.S. 284, 290 (1985).

[96] *Dr. Miles Med. Co. v. John D. Park & Sons Co.*, 220 U.S. 373, 408 (1911) (vertical agreement to fix prices); *Cont'l T.V., Inc. v. GTE Sylvania Inc.*, 433 U.S. 36, 59 (1977) (vertical customer restraint); *Monsanto Co. v. Spray-Rite Serv. Corp.*, 465 U.S. 752, 761 (1984) (vertical refusal to deal).

[97] *N. Pac. Ry. Co. v. United States*, 356 U.S. 1, 5 (1958).

[98] *Chi. Bd. of Trade v. United States*, 246 U.S. 231, 238 (1918).

[99] *Broad. Music, Inc. v Columbia Broad. Sys., Inc.*, 441 U.S. 1, 9 (1979) (citing *United States v. Topco Assoc., Inc.*, 405 US. 596, 607-608 (1972)).

A tying arrangement can violate Section 1 of the Sherman Act.[100] A tying agreement is "an agreement by a party to sell one product but only on the condition that the buyer also purchases a different (or tied) product, or at least agrees that he will not purchase that product from any other supplier."[101] One example is a company that refuses to sell replacement parts unless a customer also buys the seller's service; in this case the parts are the *tying* product and the services are the *tied* product."[102]

The Supreme Court treats certain tying agreements as illegal *per se*,[103] although there are some Justices who would prefer to apply the rule of reason.[104] The four elements of a *per se* tying violation are: "(1) the tying and tied goods are two separate products; (2) the defendant has market power in the tying product market; (3) the defendant affords consumers no choice but to purchase the tied product from it; and (4) the tying arrangement forecloses a substantial volume of commerce."[105] Courts may also take a fifth factor into account by examining whether the defendant had a strong business justification for the tie-in sale, such as a need to protect its business reputation.[106] Under the *per se* tying rule, "[w]here the conditions precedent to application of the rule are met, i.e., where the tying arrangement is backed up by the defendant's market power in the 'tying' product, the arrangement is adjudged in violation of §1 of the Sherman Act . . . without any inquiry into the practice's actual effect on competition and consumer welfare."[107]

This Note examines whether or not Microsoft's bundling of security software with the Windows operating system may constitute an illegal tying arrangement. The bulk of the discussion will relate to the Windows Firewall, which Microsoft included for free as part of Windows XP SP2. When appropriate, this Note will also discuss the Windows Malicious Software Removal Tool and the Windows AntiSpyware (Beta), which are also offered free of charge by Microsoft on their web site. In this scenario, Windows XP is considered the tying product and the firewall, malware removal tool, and anti-spyware program are the tied products.

[100] It may also violate Section 3 of the Clayton Act and Section 5 of the Federal Trade Commission Act. Although historically the three standards may have differed, today any variation in analysis is "negligible." E. Thomas Sullivan & Jeffrey L. Harrison, Understanding Antitrust and its Economic Implications 249-250 (2003).

[101] *Eastman Kodak Co. v. Image Tech. Servs., Inc.*, 504 U.S. 451, 461-62 (1992) (citing *N. Pac. Ry. Co. v. United States*, 356 U.S. 1, 5-6 (1958)).

[102] *Id.* at 460.

[103] *Jefferson Parish Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 9 (1984) ("It is far too late in the history of our antitrust jurisprudence to question the proposition that certain tying arrangements pose an unacceptable risk of stifling competition and therefore are unreasonable '*per se*.'").

[104] *Id.* at 34-35 (O'Connor, J., concurring) (arguing that tying should be analyzed under the rule of reason).

[105] *United States v. Microsoft Corp.*, 253 F.3d 34, 85 (D.C. Cir. 2001) (citing *Eastman Kodak*, 504 U.S. at 461-62; *Jefferson Parish*, 466 U.S. at 12-18).

[106] *Jefferson Parish*, 466 U.S at 34 n.1 (O'Connor, J., concurring) (referring to *United States v. Jerrold Electronics Corp.*, 187 F. Supp. 545, 559-560 (E.D. Pa. 1960), *aff'd per curiam*, 365 U.S. 567 (1961)).

[107] *Eastman Kodak.*, 504 U.S. at 487 (Scalia, J., dissenting).

B. *Application of the Per Se Tying Rule*

This section discusses the four elements of the per se tying rule as applied by the Supreme Court in *Jefferson Parish Hospital District No. 2 v. Hyde*[108] and *Eastman Kodak Co. v. Image Technical Services, Inc.*.[109] It also describes the application of the *per se* rule by the District Court for the District of Columbia in an earlier tying case against Microsoft involving the bundling of the Internet Explorer web browser with the Windows operating system.[110] Part II.C, *infra*, will discuss criticisms of the *per se* rule made by the concurring Justices in *Jefferson Parish* and by the Court of Appeals for the District of Columbia Circuit in the *Microsoft* case.

1. Separate Products

A prerequisite for finding a tying violation is establishing that there are actually two separate products whose sales have been tied. Determining the existence of separate products is not as simple as it may sound. For example, flour and sugar might be visualized as two separate products sitting in different boxes on different shelves of a grocery store. But sugar and flour may also be sold together in one box as a cake mix. In that case, their combination would constitute a single integrated product and it is doubtful that anyone would argue it is an illegal tie-in sale. The same difficulty may arise with computer software. Security software, such as a firewall, could be viewed as a separate product or as just one part of the functionality of a computer operating system.

The test used by the Supreme Court to determine if two products are distinct asks whether or not there is separate consumer demand for them. In *Jefferson Parish*, a hospital required every patient undergoing surgery to use a particular firm of anesthesiologists with whom the hospital had an exclusive contract.[111] The hospital claimed that it was “merely providing a functionally integrated package of services” and therefore it was “inappropriate to apply principles concerning tying arrangements to this case.”[112] The Supreme Court disagreed, holding that the determination of whether two products are involved does not turn on “the functional relation between them, but rather on the character of the demand for the two items.”[113] This test hinges on the perception of consumers — separate products *were not* found in a case that “did not link two distinct markets for products that were distinguishable in the eyes of

[108] 466 U.S. 2 (1984).

[109] 504 U.S. 451 (1992)

[110] *United States v. Microsoft Corp.*, 87 F. Supp. 2d 30 (D.D.C. 2000), *aff’d in part, rev’d in part, and remanded*, 253 F.3d 34 (D.C. Cir. 2001) (en banc).

[111] 466 U.S. 2 at 4-5.

[112] *Id.* at 18-19.

[113] *Id.* at 19.

buyers"[114]; yet separate products *were* identified in a sale involving "two independent transactions, separately priced and purchased from the buyer's perspective."[115] The Court emphasized that a tying arrangement could only be found where there was "sufficient demand for the purchase of anesthesiological services separate from hospital services to identify a distinct product market in which it is efficient to offer [them separately]".[116] In *Jefferson Parish*, the Court found that anesthesiology services and hospital services were two separate products that could "unquestionably" be provided separately,[117] were differentiated by consumers,[118] and were in fact sold separately by other hospitals.[119]

The Supreme Court also applied the separate demand test in *Eastman Kodak* to determine whether repair services and replacement parts constituted separate products.[120] The Court reasoned that "[f]or service and parts to be considered two distinct products, there must be sufficient consumer demand so that it is efficient for a firm to provide service separately from parts."[121] In *Eastman Kodak* there was evidence that service and parts had been and continued to be sold separately.[122] In fact, the "development of the entire high-technology service industry is evidence of the efficiency of a separate market for service."[123] The Court also rejected Kodak's argument that there could not be separate markets for the two, since there was no demand for parts separate from service.[124] Not only was that factually untrue in this case (since some services could be performed without parts) but it would also lead to an erroneous assumption that courts can never find separate markets for functionally linked articles such as "cameras and film, computers and software, or automobiles and tires."[125]

This separate demand test was followed by the district court in the tying case involving Microsoft Internet Explorer.[126] The court reiterated the Supreme Court's instructions that "product and market definitions were to be ascertained by reference to evidence of consumers'

[114] *Id.* at 19 (citing *Times-Picayune Publ'g Co. v. United States*, 345 U.S. 594 (1953)).

[115] *Id.* at 19-20 (citing *Fortner Enters. v. U.S. Steel Corp.*, 394 U.S. 495 (1969)).

[116] *Id.* at 21-22.

[117] *Id.* at 22.

[118] *Id.* at 23.

[119] *Id.*

[120] 504 U.S. 451, 462 (1992).

[121] *Id.* (citing *Jefferson Parish Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 21-22 (1983)).

[122] *Id.*

[123] *Id.*

[124] *Id.* at 463.

[125] *Id.*

[126] *United States v. Microsoft Corp.*, 87 F. Supp. 2d 30, 49 (D.D.C. 2000) , *aff'd in part, rev'd in part, and remanded*, 253 F.3d 34 (D.C. Cir. 2001) (en banc).

perception of the nature of the products and the market for them, rather than to abstract or metaphysical assumptions as to the configuration of the 'product' and the 'market.'"[127] In the case of web browsers, "the commercial reality is that consumers today perceive operating systems and browsers as separate 'products,' for which there is separate demand. . . . This is true notwithstanding the fact that the software code supplying their discrete functionalities can be commingled in virtually infinite combinations. . . ."[128]

Under the straightforward separate demand test, Microsoft's firewall, anti-spyware software, and malware removal tool constitute separate products from the operating system. There are many companies that provide security products that run on Microsoft Windows.[129] One study has predicted that the market for anti-spyware software alone is estimated to reach $305 million by 2008, up from only $12 million in 2003.[130] Because there is sufficient consumer demand for companies to provide these security software products independently of the operating system, they constitute separate products for tying purposes.

This separate demand test was rejected by the court of appeals in the Microsoft case, which criticized the test for being "backward-looking" and failing to recognize the possible efficiencies of newly integrated products.[131] This criticism will be discussed in Section II.C *infra*.

2. Market Power in the Tying Product

Establishing that two separate products exist is "only the beginning of the appropriate inquiry."[132] The next step is to determine whether or not the seller has market power in the tying product. Market power is important because it can lead to anti-competitive forcing.

> [The] essential characteristic of an invalid tying arrangement lies in the seller's exploitation of its control over the tying product to force the buyer into the purchase of a tied product that the buyer either did not want at all, or might have preferred to purchase elsewhere on different terms. When such 'forcing' is

[127] *Id.* (citing *Jefferson Parish Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 18 (1983); *Eastman Kodak Co. v. Image Tech. Servs., Inc.*, 504 U.S. 451, 481-82 (1992)).

[128] *Id.* (citations omitted).

[129] Vendors include F-Secure, Kaspersky Lab, McAfee, Symantec and Webroot. *See, e.g.*, Simon Edwards, *PC Personal Firewalls 2004*, Computer Shopper, May 2004, *available at* http://www.transceiver.co.uk/txt/pf04.html; Simon Edwards, *PC Anti-virus 2005*, Computer Shopper, Feb. 2005, *available at* http://www.transceiver.co.uk/txt/av05.html; Mary Landesman, *Spyware Stoppers*, PC World Magazine, Apr. 2005, *available at* http://www.pcworld.com/reviews/article/0,aid,119572,00.asp.

[130] Sean Michael Kerner, *Anti-Spyware Tools All the Rage*, Internetnews.com, Dec. 1, 2004, http://www.internetnews.com/stats/article.php/3442551.

[131] *United States v. Microsoft Corp.*, 253 F.3d 34, 89 (D.C. Cir. 2001) (en banc).

[132] *Jefferson Parish Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 25 (1983).

> present, competition on the merits in the market for the tied item is restrained and the Sherman Act is violated.[133]

Because an illegal tying arrangement requires "forcing," such arrangements are "condemned . . . when the seller has some special ability – usually called 'market power' – to force a purchaser to do something that he would not do in a competitive market."[134] The fear is that if market power in the tying product market "is used to impair competition on the merits in another market, a potentially inferior product may be insulated from competitive pressures. This impairment could either harm existing competitors or create barriers to entry of new competitors in the market for the tied product. . . ."[135] In *Eastman Kodak*, the Court stated that market power "ordinarily is inferred from the seller's possession of a predominant share of the market."[136]

In the case of Microsoft, both the district court and the court of appeals concluded that Microsoft had market power in the market for Intel-compatible PC operating systems.[137] In fact, Microsoft exceeded the "appreciable economic power" required by *Eastman Kodak* because it possessed actual monopoly power at the time.[138] There is evidence that Microsoft's market share in the client operating system market has actually increased since the Internet Explorer decisions were issued in 2000 and 2001. For example, a study released in 2003 said that "license shipments by Microsoft, on the client side, increased to 93.8 percent of the worldwide market in 2002, up from 93.2 percent in 2001."[139] Around the same time, "Apple's market share dropped from nearly 5 percent in 1999 to nearly 3 percent in 2001"[140] (although there has been speculation that the current popularity of Apple's iPOD portable music player may lead to increased sales of its home computers[141]). A recent report shows that Microsoft is getting increased competition from the Linux operating system, with Linux-based revenues forecasted to reach $35 billion by 2008.[142] However, even with this increase in market share by Linux, the percent of new or redeployed PCs running Linux is still only forecasted at less than 8%

[133] *Id.* at 12.

[134] *Id.* at 13-14.

[135] *Id.* at 14.

[136] *Eastman Kodak Co. v. Image Tech. Servs., Inc.*, 504 U.S. 451, 464 (1992).

[137] *United States v. Microsoft Corp.*, 87 F. Supp. 2d 30, 49 (D.D.C. 2000), *aff'd in part, rev'd in part, and remanded*, 253 F.3d 34 (D.C. Cir. 2001) (en banc).

[138] *Id.* 49 (citing *Eastman Kodak Co. v. Image Tech. Servs, Inc.*, 504 U.S. 451, 464 (1992)).

[139] IDG News Service, *Microsoft Dominance of OS Market Grows, IDC Study Says*, ITWorld.com, Oct. 8, 2003, http://www.itworld.com/Comp/2444/031008msdominate/.

[140] Jon Fortt, *Industry Awaits Taste of Fresh Apple strategy*, Chi. Trib., Jan. 5, 2003, at C-4.

[141] Wendy Tanaka, *Apple's Computers Languish Next to iPod; A Sizzling Hit - Will Music Player's Success Lead Buyers to Other Apple Products?*, Seattle Times, Dec. 20, 2004, at D1.

[142] Ed Scannel, *IDC Predicts Linux Market Worth $35 billion by 2008*, InfoWorld, Dec. 15, 2004, http://reviews.infoworld.com/article/04/12/15/HNidcforecast_1.html?OPERATING%20SYSTEMS.

worldwide by 2008.[143] At this point in time, Microsoft still has the same appreciable economic power it did in 2000-2001 when the Internet Explorer cases were decided.

3. Lack of Consumer Choice

Once it has been established that Microsoft has market power in the tying product, the next question is whether or not it is using the market power to force consumers to purchase a tied product they do not want. As the Court pointed out in *Jefferson Parish*, “there is nothing inherently anticompetitive about packaged sales. Only if patients are forced to purchase [the anesthesiologist’s] services as a result of the hospital’s market power would the arrangement have anticompetitive consequences.”[144]

At first it may seem odd to talk about “forced purchases” in the context of Microsoft’s security software, since Microsoft currently offers these products to users for free. However, this is similar to the tying arrangement found by the district court in the Internet Explorer case. The court held that there was forced bundling, even though the browser was provided for free.

> The fact that Microsoft ostensibly priced Internet Explorer at zero does not detract from the conclusion that consumers were forced to pay, one way or another, for the browser along with Windows. Despite Microsoft’s assertion that the Internet Explorer technologies are not “purchased” since they are included in a single royalty price paid by OEMs for Windows 98 . . . it is nevertheless clear that licensees, including consumers, are forced to take, and pay for, the entire package of software and that any value to be ascribed to Internet Explorer is built into this single price.[145]

Although the appeals court disagreed with the district court’s application of the *per se* rule, it acknowledged that bundling products for free could have the effect of reducing competition on the merits.[146]

> Direct competition on the merits of the tied product is foreclosed when the tying product either is sold only in a bundle with the tied product or, though offered separately, is sold at a bundled price, so that the buyer pays the same price whether he takes the tied product or not. *In both cases, a consumer buying the*

[143] IDC Software Consulting, *The Linux Marketplace – Moving from Niche to Mainstream*, Dec. 14, 2004, http://hdl.handle.net/2038/430 (access the PDF file linux_market_overview.pdf by clicking the View/Open link in the center of the page).

[144] *Jefferson Parish Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 25 (1984). However, in *Jefferson Parish* the court found that forcing did not occur. The mere preference of Jefferson Parish residents to attend the closest hospital did not prove the hospital had enough market power for the court to apply the *per se* rule when, in fact, seventy percent of patients in Jefferson Parish actually entered other hospitals. *Id.* at 26.

[145] *United States v. Microsoft Corp.*, 87 F.Supp.2d 30, 50 (D.D.C. 2000) , *aff’d in part, rev’d in part, and remanded*, 253 F.3d 34 (D.C. Cir. 2001) (en banc) (citations omitted).

[146] *United States v. Microsoft Corp.*, 253 F. 3d 34, 87 (D.C. Cir. 2001) (en banc).

> *tying product becomes entitled to the tied product*; he will therefore likely be unwilling to buy a competitor's version of the tied product even if, making his own price/quality assessment, that is what he would prefer.[147]

This same rationale applies to Microsoft's security software. Even though the firewall, anti-spyware, and anti-malware tools are provided free of charge, consumers pay for them as part of the Windows license.

In fact, the costs to Microsoft of providing free security software are arguably much higher than the costs of providing a free web browser. Security products require constant updates as new viruses and spyware are released. Microsoft itself provides an updated version of its malware removal tool on the second Tuesday of every month.[148] Security companies like McAfee and Symantec also provide frequent updates to handle new viruses.[149] The cost of performing constant research and upgrades is probably one reason why their software programs are not free.[150]

Some may argue that forcing is not a problem with Microsoft's security software since consumers are not actually forced to *use* these free products. The security software may not seem as extreme an example of forcing as Internet Explorer was — in that case OEMs and end users could not even remove the browser using the Add/Remove programs utility.[151] By contrast, consumers do not have to install Microsoft's malware removal tool or anti-spyware software. Even if users do install Windows XP SP2, they do not have to use the Windows Firewall that comes with it. The point, however, is that while consumers may not be forced to *use* the software, they have still been forced to *buy* it. Whether consumers of Windows XP decide to use the software or not, they are still *entitled to it* under their Windows licenses. All licensed users of Windows XP have paid for the right to use these products, whether they want them or not.

While it is true that some users are pleased that Microsoft is offering free security tools and feel it is "long overdue,"[152] not everyone agrees. These products are not actually "free," since their costs are bundled into the price of the Windows operating system. Many users who have Windows XP but do not trust the quality of Microsoft's current security software end up double paying: they purchase Microsoft's products as part of their Windows license, but buy

[147] *Id.* (emphasis added).

[148] Microsoft Malicious Software Removal Tool, *supra* note 54.

[149] *See, e.g.,* McAfee Recently Discovered Viruses, http://us.mcafee.com/virusInfo/default.asp?id=recentlyDiscovered (last visited Nov. 16, 2005); Symantec Latest Virus Threats, http://securityresponse.symantec.com/avcenter/vinfodb.html#threat_list (last visited Nov. 16, 2005).

[150] An annual subscription to McAfee VirusScan or Symantec's Norton AntiVirus costs $39.99. *See* McAfee Virus Scan, http://us.mcafee.com/root/package.asp?pkgid=100 (last visited Nov. 16, 2005); Norton AntiVirus 2006, http://www.symantecstore.com/dr/sat1/ec_main.entry25?page=HHONAV2006pd&client=Symantec&sid=49997&CUR=840&DSP=&PGRP=0&ABCODE=&CACHE_ID=0 (last visited Nov. 16, 2005).

[151] *United States v. Microsoft Corp.*, 87 F. Supp. 2d 30, 50 (D.D.C. 2000), *aff'd in part, rev'd in part, and remanded*, 253 F.3d 34 (D.C. Cir. 2001) (en banc).

[152] Vijayan, *supra* note 4.

other products to ensure the safety of their computers while they are online. Even if they install competing security products that are offered for free, they are still paying Microsoft for software that they do not want or need.

4. Foreclosure of a Substantial Volume of Commerce

The final step in proving a *per se* tying violation is to show that the arrangement "affects a substantial volume of commerce" in the tied product market.[153] "[N]ormally, the controlling consideration is simply whether a total amount of business, substantial enough in terms of dollar-volume so as not to be merely *de minimis*, is foreclosed to competitors by the tie."[154] In the Microsoft Internet Explorer case the district court found this threshold was met by evidence that Netscape Navigator's usage share dropped substantially from 1995 to 1998 causing it to lose advertising revenue.[155] At this point, it may be too early to tell if competing security companies have lost business to Microsoft's security software, since the firewall was only released in August 2004, the full-featured anti-virus tool is not offered yet, and the anti-spyware is still in beta testing. However, there was a dip in the stock price of at least two large competitors when Microsoft first made its announcement.[156]

It will be unfortunate if the courts wait to see substantial effects before determining whether this tying arrangement is illegal, since by that time smaller security rivals could go out of business. Even if the effects have not been felt yet, they are likely to occur as soon as Microsoft releases more full-featured products. One important thing to remember is that Microsoft has access to a distribution chain that other vendors do not have — the Windows Update utility. As commentators have pointed out, one reason Microsoft's announcement for its malware removal tool "sent shivers" through the security market was because at least 112 million PCs running Windows XP were already configured to receive updates automatically.[157] Certainly, a Microsoft distribution mechanism that pushes software updates out to millions of users has the potential to affect substantial volumes of commerce. This unique distribution mechanism in the hands of an operating system monopolist will prevent Microsoft's security products from "stand[ing] the cold test of competition" as it "insulates [them] from the competitive stresses of the open market."[158]

5. Business Justifications

[153] *Eastman Kodak Co. v. Image Tech. Servs., Inc.*, 504 U.S. 451, 462 (1992).

[154] *Fortner Enterprises, Inc. v. U.S. Steel Corp.*, 394 U.S. 495, 501 (1969).

[155] *Microsoft*, 87 F. Supp 2d at 49-50.

[156] Roberts, *supra* note 4.

[157] *Id.*

[158] *Jefferson Parish Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 12-13 (1984) (citing *Times-Picayune Publ'g Co. v. United States*, 345 U.S. 594, 605 (1953)).

The Supreme Court has allowed a defendant to make an affirmative defense to a *per se* tying claim.[159] In *United States v. Jerrold Electronics Corp.,* the Court affirmed a district court decision allowing a tying arrangement for a period of time on the grounds that it protected the seller's business reputation.[160] The district court held that the company's initial sale of complete television antenna systems was not an illegal tie, since "[t]here was a sound business reason for Jerrold to adopt this policy" because it "could not render the service it promised and deemed necessary if the customer could purchase any kind of equipment he desired."[161]

Microsoft would likely raise a similar to defense to any claim that its security offerings constitute illegal tie-in sales. It may argue that users whose computers have been infected with spyware or viruses will likely blame the operating system. For example, according to the vice president of Microsoft's Security Business and Technology Unit, one third of software crashes on Windows XP that are reported to Microsoft are caused by spyware.[162] It is understandable that Microsoft might fear that its reputation with end users will be harmed by malware infections.

However, the fact that Microsoft has security concerns does not necessarily mean that it needs to compete in the security software market. Some people argue that Microsoft could address many of those concerns by fixing security problems with Windows. One analyst from Gartner has suggested that in the next version of Windows, "Microsoft doesn't need more security -- it needs fewer security vulnerabilities. . . For [Windows Vista] to be more secure than Windows XP, it needs to be a simpler operating system -- and by jamming in more features it just raises the security risk."[163] The court in *Jerrold Electronics* was "sympathetic with Jerrold's predicament" in trying to recoup its significant investment in the development of a superior product, but did not feel that was a sufficient justification for using a tying arrangement beyond its initial inception.[164] Similarly, even though Microsoft has a valid reason to be concerned with security, that does not mean it can engage in illegal tie-in sales.

6. Conclusion of Per Se Analysis

In conclusion, there is a strong argument that Microsoft's current security offerings violate the *per se* rule against tying. First, they meet the consumer demand test that the Supreme Court uses to determine if two separate products are involved. Second, Microsoft has market power in the tying product market and exceeds the threshold requirements for a tying case since it has actual monopoly power. Third, consumers are forced to purchase these products whether they want them or not, since they are included in the cost of the Windows license. Fourth,

[159] *See Jefferson Parish*, 466 U.S. at 34 n.1.

[160] 187 F. Supp. 545, 559-560 (E.D. Pa. 1960), *aff'd per curiam*, 365 U.S. 567 (1961).

[161] *Id.* at 560. The court concluded that the arrangement was "lawful at its inception but constituted a violation of § 1 of the Sherman Act . . . during part of the time it was in effect." *Id.* at 561.

[162] Roberts, *supra* note 4.

[163] Erika Morphy, *Does Microsoft's Longhorn Mean Security Salvation?*, NewsFactor Magazine Online, Oct. 22, 2003, http://www.newsfactor.com/perl/story/22542.html#story-start.

[164] *Jerrold Electronics*, 187 F. Supp. at 561.

Microsoft's tying arrangement has the potential to affect a substantial volume of commerce. Finally, Microsoft may argue that its tying arrangement is necessary to protect its reputation, but that may not be considered a valid excuse.

C. *Analysis under the Rule of Reason*

As the previous section illustrated, Microsoft's bundling of security software with the operating system may constitute a *per se* tying violation. However, it is not clear at this time whether or not a court would actually apply the *per se* rule. In both *Jefferson Parrish* and *Eastman Kodak*, the Supreme Court continued to treat tying as a *per se* violation, but there were Justices in both cases that would have preferred to apply the rule of reason. In particular, Justice O'Connor's concurring opinion in *Jefferson Parrish* provides a comprehensive criticism of the *per se* rule on economic grounds.

In the Microsoft case, the district court followed the Supreme Court's precedent and applied the *per se* rule, but the court of appeals held that *per se* analysis was inappropriate for cases involving computer platform software. Because that issue was never reheard, we do not know if the Supreme Court would have agreed with the appellate court. If a tying case involving computer software reaches the Supreme Court in the future, the Court could very well combine the minority's earlier economic criticism with the D.C. Circuit's criticisms and decide to abandon the *per se* rule.

This section discusses criticism of the per se rule by the concurring Justices in *Jefferson Parish* and by the Court of Appeals for the D.C. Circuit in the Microsoft Internet Explorer case. It will demonstrate that their arguments in favor of applying the rule of reason instead of the *per se* rule do not apply to the security software discussed in this Note.

1. Economic Criticism of the Per Se Rule

In a concurrence joined by three other Justices in *Jefferson Parish*, Justice O'Connor criticized the application of the *per se* rule to tying cases.[165] One reason is that applying the four-part test requires much of the same effort that is expended using the rule of reason, without the benefit of allowing tying arrangements that might be beneficial to competition to be upheld.[166] She also challenged the economic basis of traditional tying doctrine. She argued that tying arrangements normally do "not increase the profit that the seller with market power can extract from sales of the *tying* product."[167] She acknowledged that tying arrangements could conceivably be "used to create *additional* market power in the market for the *tied* product," but thought that "such extension of market power is unlikely, or poses no threat of economic harm, unless the two markets in question and the nature of the two products tied satisfy three threshold criteria."[168] These criteria are "market power in the tying product, a substantial threat of market

[165] *Jefferson Parish Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 33 (1984).

[166] *Id.* at 34.

[167] *Id.* at 36.

[168] *Id.* at 36-37.

power in the tied product, and a coherent economic basis for treating the products as distinct."[169] Even if these conditions are met, however, the arrangement may not violate the law if it has economic benefits.[170]

Under Justice O'Connor's analysis, Microsoft's current security offerings would probably *not* be considered illegal tie-in sales. They would meet the first criterion, market power in the tying product, since Microsoft has actual monopoly power in the tying product. Whether they would meet the second criterion, substantial threat of market power in the tied product, is more difficult to determine. Justice O'Connor said that no substantial threat exists if there are many "stable sellers" in the tied product market or if "entry barriers in the tied-product market are low."[171] In this case there arguably is an "active and vibrant market" for Windows-based security products.[172] The real question becomes whether or not "the tying arrangement is likely to erect significant barriers to entry into the tied-product market."[173] It seems that Microsoft's ability to offer free security software that it distributes to a semi-captive audience via Windows Update is a significant barrier for new firms trying to enter the market, since no other competitor has access to such an efficient distribution chain.

However, even if Microsoft's security offerings meet Justice O'Connor's first and second criteria for finding a tying violation, they would probably not meet her third criterion, since under her reasoning they would *not* be considered separate products for tying purposes.

> For products to be treated as distinct, the tied product must, at a minimum, be one that some consumers might wish to purchase separately *without also purchasing the tying product*. When the tied product has no use other than in conjunction with the tying product, a seller of the tying product can acquire no *additional* market power by selling the two products together.[174]

The security software discussed in this paper is not something a user would purchase unless she had the tying product; it is "useless to consumers" except when used with the Microsoft Windows operating system.[175] This is also true of complementary products like cameras and film; Justice O'Connor's third criterion would allow companies to tie such functionally linked products. However, this approach was not only rejected by the majority in *Jefferson Parish*,[176] but also by the majority in *Eastman Kodak*. [177]

[169] *Id.* at 41.

[170] *Id.*

[171] *Id.* at 38.

[172] *Id.*

[173] *Id.* at 39.

[174] *Id.* (footnote omitted) (emphasis in original).

[175] *Id.*

[176] *Id.* at 19 n.30.

In addition, many of the arguments that Justice O'Connor made do not apply in the context discussed in this Note. She argued that if the tied product is useless to consumers except when used with the tying product then the seller's market power is projected into the tied product market whether the products are sold together or not, since the seller of the tying product can "exploit what market power it has . . . with or without the tie."[178] Therefore, in her reasoning, the seller will "have little incentive to monopolize" the tied product market unless it can "produce and distribute" the tied product more cheaply than others.[179]

However, Microsoft does have a reason to try to gain market power in the security market — it wants to protect its operating system monopoly. This is a concept known as *defensive leveraging*.[180] Leveraging is a concept frequently discussed in the tying context; it occurs "when a monopolist uses power in one market to induce or foreclose sales in another market and thereby monopolize both."[181] Leveraging was traditionally considered harmful because it created two monopolies and presumably more economic damage; opponents felt that "[s]urely, two monopolies generate more monopoly returns than one."[182] The Chicago school attacked this assumption by showing that a monopolist can only extract one monopoly profit.[183] Because a monopolist cannot raise prices in a secondary market without lowering prices in the primary market, "even if a monopolist gains control of a second market through leverage, the monopolist will not be able to reap additional monopoly profit."[184]

The theory of defensive leveraging provides an alternative explanation for leveraging. In this case, leveraging "is not an attempt to reap additional monopoly profit from a second market. Rather, it is an attempt to use the combined power of multiple monopolies to prevent the natural erosion of the primary monopoly."[185] There was strong evidence that this was Microsoft's motive for bundling Internet Explorer with the operating system, including memos from corporate executives specifically suggesting that the company "leverage" their operating system to get people to use their browser.[186] One author has argued that:

> Microsoft is leveraging into browsers for one key reason: to prevent browsers from eroding Microsoft's formidable monopoly in the operating systems market. This is classic defensive leveraging. A monopolist, faced with a next-

[177] *Eastman Kodak Co. v. Image Tech. Servs., Inc.*, 504 U.S. 451, 463 (1992).

[178] *Jefferson Parish*, 466 U.S. at 39.

[179] *Id.*

[180] *See* Robin Cooper Feldman, *Defensive Leveraging in Antitrust*, 87 Geo. L.J. 2079, 2079 (1999).

[181] *Id.*

[182] *Id.* at 2083.

[183] *See id.* at 2084.

[184] *Id.* at 2080.

[185] *Id.* at 2088.

[186] *Id.* at 2097-98 & 2115 n.82.

> generation product that threatens its monopoly, leverages the power from its primary market into the new market in order to protect its monopoly position.[187]

Microsoft's motivation for defensive leveraging might be slightly different in the security context than in the browser context. One motivation for defensive leveraging is the monopolist's fear that a competitor in the secondary market will develop experience, reputation, and customer loyalty that will help it to enter the primary market with a substitute product.[188] In the case of security software, it is doubtful that security companies like Symantec and McAfee will begin to compete in the operating system market. However, security problems may drive consumers to use competing operating systems such as Linux or Macintosh. As John Pescatore, a vice president at Gartner, has suggested:

> "Microsoft doesn't care about the revenue, it just wants to make it so that Windows doesn't look bad," said Pescatore, alluding to the constant barrage of media reports of spyware afflicting Windows' PCs. "They won't give it away or dump it for, say, a dollar; that would present too many political problems. But since Microsoft won't be dependent on revenues from anti-virus or anti-spyware software, they'll go after market share."[189]

Thus, Microsoft has an incentive to tie security software to the operating system, because having an entire industry dedicated to providing separate security products for computers running Windows undermines consumers' faith in the operating system and threatens Microsoft's operating system monopoly.

2. Criticism of the Per Se Rule for Platform Software

In the Microsoft Internet Explorer case, the court of appeals disagreed with the district court's finding of a tying violation and remanded to consider the facts under the rule of reason, holding that "the rule of reason, rather than per se analysis, should govern the legality of tying arrangements involving platform software products."[190]

One of the court's primary criticisms of the *per se* rule was the "poor fit" of the traditional separate-products test in the context of computer software.[191] The consumer demand test for determining separate products is supposed to "screen out false positives" by acting as a "rough proxy for whether a tying arrangement may, on balance, be welfare-enhancing, and

[187] *Id.* at 2098-99.

[188] *Id.* at 2091-92.

[189] Gregg Keizer, *Microsoft Moves on Spyware to Stymie Firefox*, TechWeb News, Dec. 17, 2004, http://www.techweb.com/wire/security/55800866.

[190] *United States v. Microsoft Corp.*, 253 F.3d 34, 84 (D.C. Cir. 2001) (en banc). Platform software is "software that serves as a platform for third party applications." *Id.*

[191] *Id.* at 85.

unsuited to per se condemnation."[192] The problem is that the test is "backward-looking" and looks at "historic consumer behavior," which makes it a poor proxy for determining whether there is "overall efficiency in the presence of new and innovative integration."[193] Although the court found that Microsoft's integration of Internet Explorer with Windows was *not* welfare enhancing (since it was used to maintain the operating system monopoly), the court agreed that "the separate-products element of the per se rule may not give newly integrated products a fair shake."[194] The rule of reason analysis allows the first company to integrate two products to show that an "efficiency gain from its 'tie' adequately offsets any distortion of consumer choice."[195]

In the context of security software, the efficiencies probably do not outweigh the negative effects on consumers. This result is counter-intuitive, since it seems logical that Microsoft providing free security software would be a boon to consumers. In the short run it may benefit consumers who do not currently use any security software at all, since using any product is probably better than none. However, in the long run consumers may be harmed if Microsoft offers free security products and drives other companies out of business without fixing the underlying security vulnerabilities of Windows. Consumers will arguably be worse off if Microsoft's competitors go out of business because their computer security will be left in the hands of the company that allowed many of the security problems to proliferate in the first place. Neil MacDonald, an analyst from Gartner, argues that "Microsoft's overriding goal should be to eliminate the need for (antivirus) and (anti-spyware) products, not simply to enter the market with look-alike products at lower prices."[196]

The court also argued that software integration should not be judged under a *per se* rule because courts do not have enough experience with arrangements involving platform software.[197] The court argued that "because of the pervasively innovative character of platform software markets, tying in such markets may produce efficiencies that courts have not previously encountered and thus the Supreme Court had not factored into the per se rule as originally conceived."[198] For example, Microsoft argued that the integration of Internet Explorer benefited third party software developers since "the bundling of a browser with OSs enables an independent software developer to count on the presence of the browser's APIs, if any, on consumers' machines and thus to omit them from its own package."[199] If one OEM failed to

[192] *Id.* at 87.

[193] *Id.* at 89.

[194] *Id.*

[195] *Id.* at 92.

[196] Munir Kotadia, *Gartner Takes Microsoft to Task*, CNET News.com, Feb. 18, 2005, http://news.com.com/Gartner+takes+Microsoft+to+task/2100-7355_3-5582742.html.

[197] *Microsoft,* 253 F.3d at 90-91.

[198] *Id.* at 93.

[199] *Id.* at 93.

bundle the browser, then some consumers might not have the APIs; thus, software developers would have to inefficiently bundle the APIs themselves with their own programs.[200]

This same rationale does not apply here, since security applications like firewalls, anti-virus, and anti-spyware software do not normally provide APIs that other parties rely on. They are software applications, not platform software. Even if they were considered platform software, there is no one security product that currently dominates the market, so third party developers should have no reasonable expectation that any particular piece of software is installed on a user's machine. Therefore, even if one agrees with the D.C. Circuit that platform software should be treated differently, the *per se* rule should still apply to the security software discussed in this Note.

In addition, even if a court does evaluate platform software bundling under the rule of reason, there are other factors it should keep in mind. Any possible efficiencies gained from tying platform software may be counteracted by other problems. First, bundling even more software with the operating system may exacerbate the network effects and increase the applications barrier to entry. Second, bundling may foreclose competition on the merits in the platform software market. Third, Microsoft could apply this argument to most software products. For example, Microsoft Word also contains APIs that developers may use — does that mean it is also platform software? Microsoft could bundle almost any software with the operating system, publish its APIs, then say that developers rely on those APIs and that it would be inefficient to unbundle them. Courts that do follow the rule of reason for platform software should balance these possible harms of platform software bundling against the alleged efficiencies.

3. Factors to Consider under the Rule of Reason

In order to prove an illegal tying arrangement under rule of reason analysis, a plaintiff must show that Microsoft's conduct unreasonably restrains competition by showing an actual effect on competition in the security software market.[201] This may require a plaintiff to define the relevant tied product market and show barriers to entry in that market.[202] A plaintiff will also have to show that Microsoft's conduct is anticompetitive and that its anticompetitive effects outweigh any procompetitive justifications Microsoft offers.[203]

In *Jefferson Parrish*, the Supreme Court held that the alleged tying arrangement did not violate the rule of reason because there was "no evidence that the price, the quality, or the supply or demand" for either the tying product or the tied product had been adversely affected.[204] For example, there was no evidence that if a patient or her doctor wanted a different anesthesiologist

[200] *Id.*

[201] *Id.* at 95.

[202] *Id.*

[203] *Id.*

[204] *Jefferson Parish Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 31 (1984).

either of them would be prevented from choosing a different one at another hospital.[205] This same analysis does not apply to Microsoft's security software. Unlike the hospital in *Jefferson Parrish*, Microsoft does have a monopoly in the operating system market, so it is not as simple for a consumer to use a different tying product. In addition, because of the price bundling, any consumer who does use Windows is paying for Microsoft's security software even if they install another company's product. This is comparable to a hospital allowing a patient to use another anesthesiologist, but still requiring the patient to pay for the hospital-recommended one.

The D.C. Circuit Court of Appeals in the Microsoft case provided a framework for determining when this type of price bundling is anticompetitive. First, a court should decide if the products actually are price-bundled by determining whether Microsoft's charge for Windows and its security products is higher than it would be for Windows alone.[206] If there is a positive price increment in Windows associated with the security software, then the plaintiff must show that the anticompetitive effects of the price bundling outweigh any procompetitive justifications that Microsoft provides.[207] In particular, the court should examine whether other operating system vendors sell their products with bundled security software.[208] If other vendors exclusively sell their products at a bundled price, then the inference is that bundled products serve consumer demand while unbundled products do not.[209]

Examining the bundling practices of other vendors with regard to security software may not be as useful as it is with regard to web browsers. Presumably, most if not all consumers who have home computers will want to browse the Internet, whether or not they are running Windows, Linux, or the Macintosh operating system. By contrast, a user's security needs may be defined by the operating system she is using. For example, a person using Linux does not have to fear the vast majority of viruses, worms, and Trojan horses that currently only threaten Windows, so it would not make sense for a Linux distributor to bundle the same type of anti-virus software that a Windows user would need. However, a user of Linux may still desire a firewall to keep out unauthorized intruders. A court would probably reach different conclusions for the different kinds of security software discussed in this Note. For example, all vendors may routinely bundle a firewall with the operating system, but not anti-virus software.

4. Conclusion of Rule of Reason Analysis

In order to prove an illegal tying arrangement under the rule of reason analysis, a plaintiff will need to show that Microsoft's security offerings unreasonably restrain competition in the security software market. At this point, the products are too new and the market is too uncertain to provide an actual, in-depth market analysis in this Note.

This section has pointed out that many of the concerns raised by Justice O'Connor's concurrence in *Jefferson Parish* and by the D.C. Circuit Court of Appeals in the *Microsoft* case

[205] *Id.* at 30 & n.50.

[206] *Microsoft*, 253 F.3d at 96.

[207] *Id.*

[208] *Id.* at 97.

[209] *Id.*

do not apply to the security products discussed in this Note. However, it seems inevitable that Microsoft will raise other arguments related to efficiency, goodwill, reputation, and consumer welfare to justify its current security software arrangements. The government did not pursue the tying claim in the Microsoft Internet Explorer case and other tying claims brought by private parties such as RealNetworks have settled, so there has been no additional guidance from the U.S. courts on software tying cases involving Windows.

III. Possible Remedies

This section discusses possible remedies if a court finds that Microsoft's security software products constitute illegal tie-in sales.

A. *Improving the Operating System*

The first option is for Microsoft to improve the security of Windows so that separate security products are no longer necessary. This is not a remedy that a court would impose, but it is something that Microsoft could do to avoid the tying issue altogether. Competing security companies may have a valid antitrust complaint if Microsoft bundles free security software with the operating system, but there is no antitrust issue if Microsoft improves its operating system so that other security products are rendered obsolete.

Microsoft has made great efforts in the last several years to increase the security of its programs, including regular briefings with security specialists and basic security training for its programmers.[210] These efforts appear to be paying off, since Microsoft has already announced several security improvements in Windows Vista.[211] Some of these changes, such as the inclusion of a firewall, arguably constitute bundling of separate products with the operating system and could possibly be challenged as illegal ties. Other security features, such as user account protection and Windows services hardening, are design changes to the operating system that do not take the place of separate products. These changes are meant to address some of the possible design flaws discussed in Part I.F *supra*, such as the fact that many Windows programs require administrative privileges to run. It is not clear at this point whether these changes will be enough to make separate security products unnecessary.

B. *Releasing Different Versions of Windows*

The second option is for Microsoft to provide two versions of Windows — a bundled version that includes security tools and an unbundled version for users who want alternative security products. This is the remedy that the European Union has imposed on Microsoft in a

[210] John Markoff, *At Microsoft, Interlopers Sound Off on Security*, N.Y. Times Online, Oct. 17, 2005, http://www.nytimes.com/2005/10/17/technology/17hackers.html.

[211] Microsoft Windows Vista Security, *supra* note 71 (describing various security features of the Windows Vista architecture).

case involving Windows Media Player; Microsoft has released a stripped down version of Windows called "Windows XP Home Edition N," which does not come with a media player.[212] Whether this is an appropriate remedy for security software may become increasingly important, since it appears that the European antitrust authorities are starting to investigate Microsoft's bundling of security software with Windows Vista.[213]

From a consumer standpoint, the remedy imposed in the media player case may seem strange since the version without the media player costs the same amount as the regular version. However, even though this unbundled version may not save consumers any money, it levels the playing field by allowing for unbridled competition among media player vendors. In the end, this will likely lead to vibrant competition and better choices for consumers in the media player market.

In the security software scenario discussed in this Note, there is an additional component of consumer harm. As discussed in Part II.B.3 *supra*, many users who do not trust Microsoft's security offerings end up paying double — first, for Microsoft's security products as part of their Windows license and second, for separate security products from other vendors. For these unsatisfied users, unbundling will only be an attractive remedy if the unbundled version costs less, so that they can spend the money saved on alternative security products.

Microsoft may argue that this is an extreme and inefficient remedy for a tying violation. If Microsoft took this approach with all products (e.g., browsers, media players, firewalls, text editors, photo viewers, etc.), it would result in the release of dozens of versions of Windows with different configurations. Consumers would likely be confused, and the price of Windows would probably go up to pay for the extra marketing, development, and packaging of the different product configurations.

However, there is an even stronger argument for requiring Microsoft to unbundle its security software than its media player or web browser: the nature of the software is different. People use media players to watch videos or listen to music, and they use web browsers to surf the Internet. They can install several different media players and browsers on their machine, whether or not one comes bundled with Windows. But people do not buy security products for fun and entertainment; they *need* them to protect their Windows machines from malicious software. For technical reasons, it is impossible to run two different firewalls on one personal computer (the same is true for some anti-virus products, but not for most anti-spyware programs). If the Windows Firewall comes bundled with Microsoft Windows Vista, then users who do not want it will have to disable it to use other software; they cannot run a competitor's firewall at the same time.

C. *Releasing Separate Security Products*

The third option is for Microsoft to offer its security software as separate paid products, as competing security companies like Symantec and McAfee do. Microsoft appears to be

[212] Ina Fried, *Microsoft to Rename Media-Player-Less Windows*, CNET News.com, Mar. 29, 2005, http://news.com.com/Microsoft+to+rename+media-player-less+Windows/2100-1014_3-5643117.html.

[213] Kirk, *supra* note 15.

leaning towards this third approach, as it conducts beta testing of software products like Windows OneCare and Microsoft Client Protection. Microsoft does have a valid interest in computer security and should be allowed to develop its own security products such as firewalls, anti-virus, and anti-spyware software. However, Microsoft does not have a right to use illegal tie-in sales to force consumers to buy products they do not want. Under this third approach, Microsoft's security products will "stand the cold test of competition" on the merits in the market.[214]

This approach may foster the most competition and provide the best choices for consumers in the security software market. As discussed in Part I.F *supra*, there are at least two possible reasons why users need security software when running Microsoft Windows: (1) design flaws in Windows, and/or (2) attention from malicious software writers due to the popularity of Windows. If one believes that Windows has design flaws, then it is especially important that other companies, who understand security better and are less likely to make the same mistakes, provide these products. Under this theory, Microsoft should expend its development resources trying to fix the vulnerabilities that allow these security problems to occur, rather than driving away competitors with free or low-cost security products that are shielded from competition on the merits but do not effectively protect consumers.

If one believes that Microsoft Windows is not inherently flawed, but is just a popular target for malicious intruders, it is still important to have other security companies provide these products. As long as Microsoft retains its operating system monopoly, it will be a target for malicious software writers and computer criminals. It is important to maximize the amount of people working to counteract this negative network effect. If competing companies go out of business, there will be less resistance to malicious intruders and consumers will be the ultimate victims.

Conclusion

As the beginning of this Note discussed, Microsoft has shaken up the computer software industry with its entry into the security software market. This is a time of great change, with news articles announcing new product offerings by Microsoft and its competitors on an almost daily basis. There is a strong argument that Microsoft's bundled security offerings may constitute a *per se* tying violation under Section 1 of the Sherman Act. However, it is not clear whether a court hearing a case today will actually apply the *per se* rule. If a court instead decides to apply the rule of reason, the outcome is very uncertain. Although many of the justifications that Microsoft provided in the Internet Explorer case do not apply to security software, the company may invoke other efficiency arguments that courts will embrace. If a court does find a violation, there are several available remedies, one of which is to require Microsoft to release different versions of Windows, both with and without added security features.

[214] *Jefferson Parish Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 12 (1984).