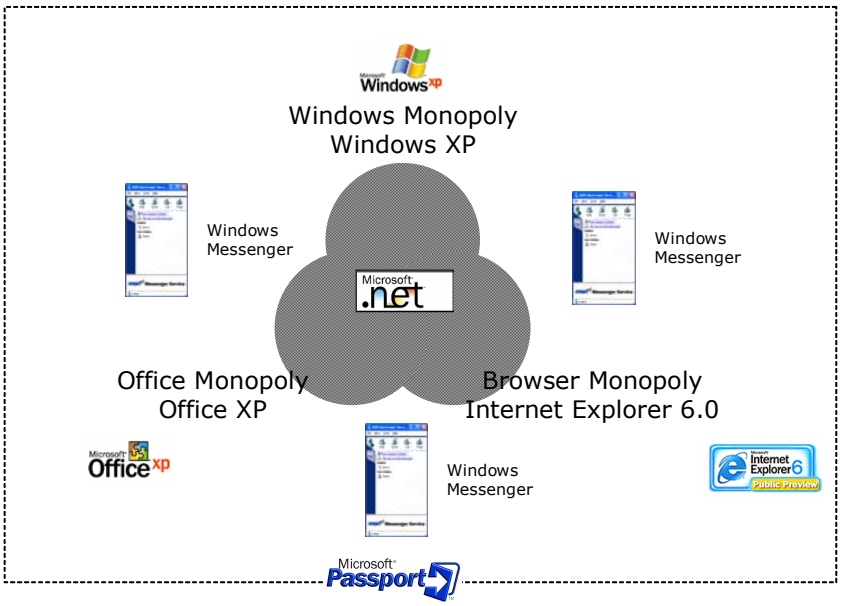
ProComp

Project to Promote Competition and Innovation in the Digital Age

PASSPORT TO MONOPOLY

WINDOWS XP, PASSPORT, AND THE EMERGING WORLD OF DISTRIBUTED APPLICATIONS

June 21, 2001



2001 K Street, NW, Suite 800
Washington, DC 20006
www.procompetition.org
(202) 912-7140

TABLE OF CONTENTS

In October 2001, Microsoft is scheduled to release Windows XP, the most important new release of Windows since Windows 95.[1] Windows XP raises many important antitrust and public policy issues that are beyond the scope of this paper. The purpose of this analysis is to focus specifically on three issues that are unlikely to be addressed by resolution of the appeal in *United States v. Microsoft*. First, it discusses the significance of a new class of "distributed" applications that promise to revolutionize Internet communications and commerce; second, it addresses how Microsoft is using Windows XP and its new browser monopoly to gain control of these new "killer" applications, thereby raising important remedial issues in the event that Microsoft is found to have illegally maintained its Windows monopoly or obtained its browser monopoly; and third, it describes how Microsoft's conduct in bolting its distributed applications to Windows XP appears to go well beyond the standard urged by Microsoft itself in the pending litigation, and hence to raise important antitrust issues even in the unlikely event that it is found not to have violated the Sherman Act with respect to the pending case.

I. INTRODUCTION

A new class of "distributed" applications are likely to revolutionize Internet communications and commerce over the next two to three years. Two types of distributed applications are particularly important: instant messaging, which is being transformed from simple text "chat" into a powerful communications tool with better-quality voice and more powerful features than the traditional telephone; and Web services, which provide services to enable instant commerce. One respected analyst firm recently compared the importance of these emerging instant messaging and

---

[1] *See, e.g.*, Jay Greene, *Microsoft: How it Became Stronger Than Ever*, Business Week (June 4, 2001), at 76.

Web services to the invention of the automobile assembly line[2]; whether that proves to be the case or not, there appears to be broad consensus that these distributed applications will match if not eclipse in significance the desktop applications that Microsoft has monopolized with Microsoft Office.

If instant messaging and Web services are the new "killer applications," a specific Web service known as an "identity service" will be of crucial importance in accessing those services. In order to communicate or engage in commerce over the Internet, it is necessary for the user to be able to establish their identity; conversely, once the user's identity is established, it is possible to deliver a host of other Web services to that user. The result, as one analyst observed, is that "instant messaging battles will lead to identity wars." Identity will be invaluable to competitors because consumers and business users "may be pledging not only their IM address, but also their future online persona and personal data":

> This long-term market advantage will be far more beneficial than owning an e-mail address or domain. Instant messaging will be the core of wireless e-commerce, live collaboration, virtual gaming and a host of other Internet applications. "As you select your instant messaging preference, think about who will safeguard your banking data, social security number and a host of other private transactions," said Neil MacDonald, Gartner analyst.[3]

The platform for invoking these new distributed applications in effect is the technology at issue in the pending case of *United States v. Microsoft*. As Windows XP itself makes clear, and as

---

[2] Gartner Press Release, *Gartner Examines Microsoft Versus America Online Impending War in Instant Messaging and Web Services Space* (May 1, 2001) (analogy by Gartner Vice President David Smith), *available at* http://www4.gartner.com/5_about/press_room/pr20010501a.html.

discussed in the pages that follow, the principal user interface (that is, the screen display) from which the user accesses these services will be the browser; and the principal program interface (that is, the application program interfaces, or "APIs," that the application developer invokes) is a run-time environment like Java.

Microsoft's plan for maintaining and extending its desktop monopoly to these new applications and to the applications platform has been is known as Microsoft's ".NET initiative." According to Microsoft's Web site, .NET is "an operating system for the Internet," designed to replace the Internet's current "disjointed, disparate, fractured environment" with "a common infrastructure with one model of developing for it."[4] This "common infrastructure," in Microsoft's plan, will be a proprietary platform that Microsoft owns and controls, just as Windows is today. As Microsoft Chairman Bill Gates explained in a recent interview:

> Q: [I]s .NET a platform-independent strategy?
>
> A: No. No. .NET is a Microsoft platform. Just like the Windows platform. Windows was built on common standards, like standard character sets like TCP/IP. It was all built on standards. But it was a Microsoft platform too. .NET is a Microsoft platform. We haven't decided Microsoft is a zero-revenue company. [Becoming animated] We're spending $3 billion a year. Listen: the way we do handwriting recognition; the way we do speech recognition; the way we do speech recognition; the tools that we create; the user interface; the office productivity apps -- those will be

---

[3] Gartner Press Release, *Gartner's Instant Message Survey Shows America Online Leading Microsoft* (May 1, 2001), *available at* http://www4.gartner.com/5_about/press_room/pr20010501b.html.

[4] *Web Services, an Interview with Robert Hess* (Mar. 19, 2001), *available at* http:\\www.Microsoft.com/business/vision/hess_on_web_services.asp.

> built around .NET. That's a capitalistic act. OK? I don't know anybody ever got confused about that.[5]

Microsoft's .NET initiative thus is not an "open systems" deviation from its Windows model. To paraphrase Mr. Gates, Windows is not "open" simply because it uses TCP/IP, and .NET similarly will not be "open" simply because it uses XML. To the contrary, .NET is best understood, in the words of Microsoft's .NET white paper, as "the next generation of the Windows desktop platform"[6] -- and, as Microsoft has been equally forthright in explaining, it represents Microsoft's initiative to obtain the same kind of hold over the Internet that it currently exerts through Windows over the PC desktop.

The remainder of this white paper describes how Microsoft intends to obtain such control through the release of Windows XP. The white paper focuses in particular on how Windows XP is designed to force adoption of Microsoft's Web services, known as "Hailstorm"; its instant messaging program, known as MSN Messenger; and, most of all, its identity service, known as Microsoft Passport. For example, Microsoft has bolted Microsoft Passport to the forthcoming Windows XP in a way that appears to violate even the standards that Microsoft advocates, and may be viewed as having improperly "exploit[ed its] dominant position in one market to expand [its] empire into the

---

[5] *Bill Gates Unplugged*, Redherring.com (Sept. 2000), *available at* http:\\www.redherring.com/mag/issue82/resources/mag-gates-82-p3.html. The observation about Mr. Gates' demeanor is by the interviewer.

[6] As Microsoft Chairman Bill Gates has explained, "there's a very strong analogy here between what we're doing now and what we did with Windows. . . . So for every element of Windows -- user interface, the APIs, the hardware drivers that allowed it to work with all the different capabilities people plugged into the PC -- for each one of those things there's an analogy here." Bill Gates,

next." *Eastman Kodak Co. v. Image Technical Services, Inc.*, 504 U.S. 451, 498 (1992) (Scalia, J., dissenting).

Moreover, Microsoft's conduct implicates privacy and public policy concerns that go beyond the antitrust laws. If allowed to monopolize Web identity through Microsoft Passport, Microsoft has announced that it plans to collect and use information about users in a fashion that goes well beyond anything ever contemplated by any private business. Microsoft also has shown, through technologies incorporated into Windows XP, that it intends to use its monopoly control of the Internet in a way that enables it to appropriate and alter third-party content without the consent of the content creator.

The remainder of this white paper proceeds in four parts. To begin, Section II discusses why, as a result of broadband connections that take greater advantage of the Internet's underlying architecture, the Internet revolution is only in its beginning stages. The significance of the new category of "distributed" applications that has emerged as a result is difficult to overestimate: as the *New York Times* recently observed, the "range of distributed applications that may emerge within a decade and affect society is almost limitless." [7]

As the name suggests, "distributed" applications do not reside principally on a single computer, but rather are "distributed" across multiple machines on the network. Two types of distributed applications are likely to be particularly important to consumers: those that enable

---

Forum 2000 Keynote: Bill Gates Speaks About the .NET Platform, *available at* http://www.microsoft.com/BUSINESS/vision/gates.asp.

communication (such as instant messaging) and those that facilitate the delivery of goods and services ("Web services"). Instant messaging, which allows for the instantaneous communication of text, voice, and video, is by some accounts growing faster than any communications medium in history.[8] Web services can be expected to become similarly pervasive, as they enable the delivery of customized information to consumers regardless of whether they access the information from home, the office, or some other location.

Because distributed applications are not tied to a particular machine, access to these services depends in the first instance on establishing the user's proper identity. Whether the user wants to place an Internet telephone call, or purchase tickets from an online travel agency, it is first essential to establish that the user is who the user claims to be. Web identity and authentication services accordingly will be the key user point of access to distributed applications on the Internet. As Microsoft observes with regard to its own Web identity service, Microsoft Passport, "Passport is the key to enabling this collaborative experience in the .NET environment."[9]

Section III explains how Microsoft intends to use its forthcoming Windows XP operating system to ensure consumer adoption of its own distributed applications. To begin with, Microsoft

---

[7] J. Markoff, *Software's Next Leap is Out of the Box*, N.Y. Times (E-Business Special Section), June 13, 2001.

[8] The market research firm Gartner Group, for example, estimates that the number of instant messaging users will grow to more than 180 million by 2004, by which time 60 percent of all real-time online communication -- voice or text -- will be driven through instant messaging technology. Gartner Press Release, *Gartner's Instant Message Survey Shows America Online Leading Microsoft* (May 1, 2001), *available at* http://www4.gartner.com/5_about/press_room /pr20010501b.html.

[9] *Microsoft Passport: A Key Component of the .NET Vision*, http:\\www.microosft.com/msdn-online/start/features/passport.asp.

has made Microsoft Passport the exclusive Web identity service that Windows XP will support. As one industry analyst observed, Microsoft easily could have chosen to allow selection from competing identity services, but it simply "has chosen not to do this," because "Microsoft regards Passport as a key leverage point and will use its own established platform dominance to drive exclusive usage."[10]

To the extent that Microsoft intends to defend Passport exclusivity on the same "integration" grounds that it used with Internet Explorer, this argument is unavailing. In fact, a Web identity service and a desktop operating system are more than simply unrelated -- they are *antithetical* in their functionality. The purpose of an identification service is for a neutral party (such as Microsoft) from servers at some unrelated location on the Internet (such as Redmond, Washington) to confirm to a third party (such as a commercial Web site) that the user is who the user claims to be. The identity/authentication service (and the process it uses to confirm identity) must be separate from (not integrated with) the user's desktop or other client machine. It is therefore difficult to imagine products that are less desirable to "integrate" than a desktop operating system and a Web identity/authentication service.

Section III shows that Microsoft also is using Windows XP -- and, more particularly, Internet Explorer -- in other ways to create bias in favor its own distributed applications. As the design of Windows XP itself attests, the browser (Internet Explorer) rather than the desktop operating system (Windows) is the natural user interface from which users will access this new universe of distributed

---

[10] David Smith and Chris LeTocq, *Commentary: Hailstorm's Consumer Focus*, Gartner Viewpoint, CNET News.com (Mar. 20, 2001), *available at* http://news.cnet.com/news/0-1003-201-5195835-0.html?tag=lh?tag=st.ne.ni.gartnerbox.gartnercomm.

applications. If there were still competition in the browser market, Microsoft's control of the user interface would be under threat. Having eliminated any such competition, however (Internet Explorer's market share is now more than 85%[11]), Microsoft benefits both through the maintenance of its platform monopoly, and the chance to monopolize the distributed applications for which the browser is the user interface.

Section IV shows that Microsoft's conduct cannot be squared with the antitrust laws under the standards articulated by Microsoft in *United States v. Microsoft*. Moreover, Microsoft's conduct raises significant issues that extend beyond the antitrust laws. First, if Microsoft is permitted to gain an identity monopoly, it will raise privacy and security issues that dwarf those previously raised by Internet technologies. Through Passport and its related Web services, Microsoft has announced that it will develop a centralized database containing all of the information provided by users to any Passport Web site (which, if Passport becomes the monopoly Web identity service, will be virtually every Web site). Unlike most of the information presently supplied by users browsing Internet sites, the information Microsoft collects and controls will be personally identifiable to the user; and, as a result of gaps left open in Microsoft's "privacy policy" (which Microsoft expressly has said may be changed at any time), Microsoft will have few restrictions on its ability to use this information as it sees fit. At the same time, the breadth and scope of information that Microsoft seeks to collect is striking:

---

[11] *See, e.g,* WebSideStory StatMarket Press Release, *Microsoft's Share of Browser Market Continues to Rise: Now More Than 87%* (Feb. 22, 2001), *available at* http://www.websidestory.com /cgi-bin/wss.cgi?corporate&news&press_1_104.

> Microsoft wants to know everything: the information in your user profile, address, and application settings; what devices you use; what's in all your documents; your favorite Web sites; where you are at any given moment; your credit card numbers and payment information; the contents of your personal calendar, contact list, and e-mail inbox; and probably a few things I've left out.[12]

Microsoft's monopoly control of the browser user also raises serious issues of a broader nature -- issues exemplified by SmartTags, a technology that Microsoft has employed with Internet Explorer as a means of biasing the display in favor of its own distributed applications and other online services. Through SmartTags, Microsoft is able to scan and edit the content a user chooses to view, adding its own links into that content. Users of Microsoft Word who are familiar with the red squiggly lines automatically generated by its spellchecker will recognize the technology: now, with Internet Explorer in Windows XP, purple squiggly lines will appear under words where Microsoft has created links to Microsoft Web services and sites. So, for example, if the user is reading a *Washington Post* article online, the browser might add a purple squiggly line under the name of a person that links to the relevant Microsoft Encarta biography entry; a company name might link to the Microsoft MSN MoneyCentral financial service.

The potentially problems raised by SmartTag and other Internet technologies do not result from the technologies themselves. The concerns arise instead from the likely monopoly control of these technologies by one company, under circumstances where the power of the technologies amplifies their potential for misuse through the invasion of privacy or control over third-party

---

[12] David Coursey, *.Net Demystified: What You Must Know About MS's Software Scheme*, ZDNet (Mar. 20, 2001), *available at* http://www.zdnet.com/anchordesk/stories/story/0,10738,2698647,00.html.

content. As the *Wall Street Journal*'s personal technology column recently summarized with respect to SmartTags:

> There have been some excellent third-party programs, like GuruNet (now Atomica), that let users click on words within Web pages to get more information. But these don't place new links on pages, and they aren't built into the browser that more than 80% of Web visitors use.
>
> Microsoft's Internet Explorer SmartTags are something new and dangerous. They mean that the company that controls the Web browser is using that power to actually alter others' Web sites to its own advantage. Microsoft has a perfect right to sell services. But by using its dominant software to do so, it will be tilting the playing field and threatening editorial integrity.[13]

Finally, Section V addresses potential responses to Microsoft's most recent conduct. In that regard, it would appear that conduct remedies are unlikely to be effective. For example, there is a court order in place prohibiting Microsoft from bolting products to Windows. This consent order was agreed to by Microsoft in connection with the Justice Department's lawsuit against the company in 1994. Since that time, the number and variety of products and services that Microsoft has bundled with Windows reflect the enormous difficulty in attempting to proscribe specific conduct in a way that is effective in remedying conduct determined to be anticompetitive.

A structural remedy along the lines proposed by the District Court in the *United States v. Microsoft* browser litigation, but which separates Internet Explorer from Office, may be more effective as a means of preventing Microsoft from extending its browser monopoly into distributed applications and other online services. In this respect, it is notable that the only serious rival to

---

[13] Walter Mossberg, *Dangerous Detours: Windows XP May Add its Links to Others' Sites*, Wall Street Journal, June 7, 2001, at B1.

Internet Explorer as a platform for distributed applications appears to be Microsoft Office. The enormous projected increase of instant messaging in the workplace, together with Office's large installed base, potentially would make an Office company a formidable rival to -- and alternative platform for competitors of -- Internet Explorer and Windows.

Delay in the imposition of an effective remedy, by contrast, may make Microsoft's monopoly increasingly difficult to unwind. If Microsoft succeeds in expanding from a product to an additional service monopoly, it is likely to make its monopoly even more durable. Microsoft will not be subject to further upgrade cycles, and users are likely to be locked into this identity service in the same way (though to a greater extent than) users today get locked into their email identity. Moreover, Microsoft's monopoly is likely to expand further, not just into distributed applications and online services, but into all server software as well. The reality today is that server software is dependent upon compatibility with client software, not unlike the way that desktop applications today are dependent upon the desktop operating system. Microsoft may have already achieved monopoly or near monopoly power in the low end of the server market through its proprietary connections between its desktop operating system and its low end servers. Microsoft is expanding its presence into those markets at a rapid pace,[14] and if Microsoft obtains a monopoly in distributed applications, this process is likely to accelerate.

---

[14] IDC Press Release, *Microsoft Strengthens Its Grip, Narrowing the Window of Opportunity for Other Operating Environments* (Feb. 28, 2001), *available at* http://www.idc.com/software/press/PR/SW022801pr.stm ("[D]uring 2000, Windows strengthened its hold on both the desktop and server. According to IDC, Windows accounted for 41% of server operating environment (SOE) shipments and an overwhelming 92% of shipments for the client operating environment (COE).") And Microsoft's share of the low end server market is significantly higher.

* * * *

Microsoft's forthcoming release of Windows XP appears to constitute a significant event in the evolution of the Internet. Microsoft has made no secret of the fact that it would like to control the means by which users access the Internet, and the distributed applications that they employ. Given the important public policy consequences that arise if Microsoft succeeds, and the likelihood that it will do so, the issues raised by the release of Windows XP warrant careful review.

II. THE REVOLUTION CONTINUES

In the past few years, Americans' use of the Internet has skyrocketed. According to a Zogby poll conducted in March 2001, 71% of adult Americans now report having access to the Internet -- virtually the same number as the 72% who report owning a PC. In August 1997, by contrast, three and a half years before, only 16% of respondents reported having access to the Internet.[15] Moreover, Americans do not simply have access to the Internet; they also use it. In the Zogby survey, 81% of those with access to the Internet used it for at least one hour a week.

As remarkable as these numbers are, they are in all likelihood only the beginning of the Internet revolution. In the 1990's, PCs were connected to the Internet through hardware connections

---

[15] Zogby International Press Release, *New Zogby "Tech Watch" Poll Reveals: Three in Four Now Have Internet Access* (Mar. 22, 2001), *available at* http://www.zogby.com/news/ ReadNews.dbm?ID=359. As a point of reference, it is notable that 72% of Americans in the survey reported owning a PC in March 2001 -- almost exactly the same percentage as those reporting access to the Internet. *See Zogby's Latest Exclusive Report: TechWatch 1994-2001* (April 30, 2001), *available at* http://www.zogby.com/news/ ReadNews.dbm?ID=376#Anchor-Te-31055.

that restricted their ability to take advantage of Internet technology. The recent spread of high-speed Internet service, however,[16] has given rise to a whole new category of "distributed" applications that take advantage of the Internet's underlying architecture.

As discussed in the section that follows, two features of distributed applications in particular constitute a revolutionary change from the previous "client-server" model. First, rather than residing principally on one machine (either a client or a server), distributed applications effectively reside on the network itself -- "in the cloud," in the terminology of some in the computer industry. It is therefore possible to access these floating services from any computer connected to the Internet. Second, because the applications and data are accessible from different machines, access to these services depends critically upon being able to establish the identity of the user seeking access to those services. Web identity and authentication accordingly assume great importance in a world of distributed applications.

Two types of distributed applications already have been introduced and rapidly are assuming considerable importance: instant messaging ("IM"), which rapidly is evolving beyond text to include real-time voice and video communications; and Web services that allow for the customized and integrated delivery of online services and other transactions. This section begins with a general discussion of the Internet's underlying architecture and the means by which distributed applications

---

[16] Forrester Research estimates, for example, that nearly half (47%) of Internet access will be at broadband speeds within the next three years. *See* Lee Bruno, *It's Official: The PC is No Longer the Province of One Machine*, Red Herring (Mar. 6, 2001), at 90. Broadband connections not only are capable of carrying far greater volumes of information than the modems of the mid-1990's, but they are also "always on," meaning that they require no dial-up or lengthy connection procedure.

take advantage of that architecture; and then turns to a brief discussion of how distributed applications will revolutionize the efficiency and power of online computing.

A. The Internet: its Origins and Extension to PCs.

The Internet is a global web of computer networks whose origins date back to the early 1970's, when military researchers sought to devise a system that would ensure that computers in this country would not be susceptible to significant disruption in the event a single computer or a single connection were destroyed. To facilitate this goal, they decided that the system should not be set up as a single network, in which a central computing facility would handle network management functions, such as ensuring data security and integrity and routing data to the appropriate network nodes. Instead, they sought to devise a network of networks, in which there is no central management.

For such a system to work, the participating networks had to be able to communicate and exchange data among themselves, regardless of the fact that the participating networks might employ different kinds of computers. Ian Kahn and Vinton Cerf eventually devised two open "protocols" to enable such communication: a network protocol, called the "Internet Protocol" ("IP"); and a transport protocol, called the Transport Control Protocol ("TCP"). Often the two protocols are referred to together as TCP/IP. At the beginning of 1983, the military required every computer in the network to use TCP/IP, and the network of computers linked through TCP/IP was named the "Internet."

One of the powerful characteristics of networks based on TCP/IP is that computers are "peers" -- that is, each computer is capable of initiating and responding to requests. This relationship

is different, for example, from traditional client-server networks, in which the client's requests typically are fulfilled by an application server residing on a centralized computer. Although TCP/IP applications can easily be used in a client-server setting, the Internet enables a wide range of additional capabilities that simply are not possible in most conventional client-server networks. Instead of being limited to the computing resources of one computer, for example, programs can be "distributed" across hundreds or thousands of computers, with the components of the program interoperating in much the same way as they would if they all resided on the same computer.

There is no architectural reason why PCs and other computing devices cannot be incorporated into the TCP/IP network as "peers," and hence capable of participating in a distributed computing environment. Indeed, because the TCP/IP protocols were designed for use by different computer platforms, the Internet's architecture is naturally suited to the addition of new types of computing devices quite unlike the large-scale computers for which the Internet originally was conceived. In order to be able to function effectively in a distributed environment, however, the PC's connection to the Internet must be capable of carrying a considerable volume of data. Until recently, low-speed dial-up modems were capable of supporting only a limited amount of data exchange.[17]

Software developers responded to these limitations in the 1990's by focusing on Internet applications that simply required the delivery of largely passive data (for example, web pages and

---

[17] Moreover, PCs were not connected permanently to the Internet, but would enter and leave frequently and unpredictably, with continually changing IP addresses. Prior to the advent of the Web, computers on the Internet responsible for software applications were assumed to be substantially always on and always connected, and the fixed address system that had been devised for Internet computers under such circumstances was not well-suited for this kind of activity.

email messages) from servers on the Internet. In such applications, the PC is not operating much differently from a "dumb" client requesting data over a traditional client/server network. In some respects, therefore, Internet usage via Web browsers and email has not really even begun to tap into the extraordinary potential computing capabilities provided by a network that now comprises tens of millions of computers.

B. The Advent of Distributed Applications

With the increasing adoption of high-speed "broadband" technologies such as DSL, cable and wireless, PCs increasingly are able to function as true "peers." Broadband connections are capable of carrying far greater volumes of information than the modems of the mid-1990's, and they are "always on," meaning that they require no dial-up or a lengthy connection procedure. As a result, PC users increasingly are able to access distributed applications from their desktop. From the user's perspective, although the application itself resides on the network, it is accessible as rapidly and seamlessly as if it resided on the user's own PC.

The ability of PC users to access distributed applications has generated an enormous rush to develop applications that bring this functionality to the user's desktop. As the *New York Times* recently explained:

> Some software designers call it moving off the desktop and into the cloud. Traditionally, software has been a product, code stored in a single disk or CD that is loaded into an individual machine. Software companies large and small are now working to transform it into an array of floating services available through a global network of computers woven together from high-speed networks of copper, fiber-optic glass and radio waves. . . . Perhaps the best example of the power of distributed computing is in the Internet's domain name system. It is, in fact, a vast database that exists on many servers and instantly provides address information to any computer connected to the Internet. However, the range of distributed

> applications that may emerge within a decade and affect society is almost limitless, stretching from energy management to traffic control systems.[18]

As software moves "into the cloud," it obviously becomes necessary to be able to determine how to control access to the applications and data of a particular user. Notably, there is nothing in the Internet's design that requires the delivery of this information to a particular *machine* rather than a particular *user*. Indeed, in 1996, the Israeli software company ICQ ("I seek you") developed a directory of Internet addresses that are identifiable to particular user identities. By devising a directory that can update IP (the "IP" in "TCP/IP") addresses in real time, the user's "presence" on the Internet can be established from any device.

By rough analogy, Web identity and authentication might be thought to serve the same function as a bank customer's ATM card and password. Just as an ATM card and password enable a bank customer to obtain account information and carry out banking transactions from anywhere in the banking network, so too Web identity and authentication will enable the computer user to access distributed applications and services from any device connected to the Internet. In the next few years, two sets of services are likely to be particularly important: real-time communication, through the continued development of instant messaging technology; and applications that enhance the speed and efficiency of online commerce.

C. Instant Messaging and Web Services

---

[18] John Markoff, *Software's Next Leap is Out of the Box*, N.Y. Times (June 13, 2001) (E-Business Special Section).

Instant messaging enables online users to communicate instantaneously with each other, either one-to-one or in a group. Instant messaging first came into use on the Internet in the late 1980's, and initially constituted only a modest advance on traditional email programs. It began to be used more widely after America Online introduced the "buddy list" (or "presence management") in 1996. Presence management works like an interactive address book, which lights up a user's name when the user has contacted a server using specialized client software that registers the user as being online.

So long as instant messaging was limited to text-based, email-like messages, however, its use remained confined principally to free, online "chat." Indeed, only approximately 5.5 million users used IM in their workplace in 2000. With the increasing deployment of high-speed Internet service, however, IM can carry higher-bandwidth communications (like voice), and the use of IM as a major communications tool is expected to explode. The research firm IDC, for example, expects corporate use of IM to grow by 140% a year for each of the next three years, to 180 million users in 2004.[19] Gartner Group expects a similarly explosive rate of adoption, projecting that by 2004, fully 60% of real-time communication between users via any means (including voice, text, and call-response), will be driven through IM technology.[20]

---

[19] IDC Press Release, *Corporate Instant Messaging Will Grow at a Strong Rate but Faces Obstacles* (Oct. 24, 2000), *available at* http://www.idc.com/software/press/PR/SW102400pr.stm.

[20] Gartner Press Release, *Gartner's Instant Message Survey Shows America Online Leading Microsoft* (May 1, 2001) (AOL has 51% consumer market share versus 36% for Microsoft; and 52% business market share compared to 40% for Microsoft), *available at* http://www4.gartner.com/5 about/press_room /pr20010501b.html.

Fueling this projected rate of adoption are two important advances in IM. First, as broadband Internet connections become commonplace, PCs will be able to support the real-time exchange of voice and video as well as text messages. When combined with "presence management" and the location independence of distributed applications, IM will be able to deliver voice (and, eventually, video) communication service that is superior to the telephone network. As John Markoff recently explained in the *New York Times*:

> In the future, not only will Internet telephone calls be higher quality than on today's telephone network, but the personal computer will offer new features like the ability to tell whether the person being called is at her desktop computer before the call is made and "follow-me" capabilities that let the network track a person's location whether she is at the desk, at home or reachable by cellular telephone.[21]

Moreover, IM will not simply deliver superior telephone and video service. An important reason for its likely widespread adoption in the workplace is that it will dramatically enhance the ability of business colleagues to engage in collaboration and coordination tasks. For example, distributed computing makes it possible to engage in real-time collaboration in which all members of a business team can work on the same document at the same time. The document appears in a group "workspace" accessible to all members, and each person can make mark-ups to the document that are immediately seen by all of the members of the group. Other members can ask questions or make further changes until a final version is complete.

The dramatic expansion in the scope and use of IM is likely to be paralleled by the rapid adoption of a new class of distributed applications referred to as Web servoces/ Web services

provide information from a server residing on the Internet in response to a request from an Internet client. For PCs connected to the Internet through an "always on" connection, Web services can automatically provide the user with dynamically updated information, such as stock tickers, weather and travel updates, and news.

In providing such information, Web services do not have to be accessed by the user directly. They can also be accessed -- and increasingly will be accessed -- through client "scanning" software, such as that developed by GuruNet (now Atomica) and Firefly (now owned by Microsoft). Scanning programs run in the background when the user is running another application program (for example, a browser or word processor). Using technology similar to that used in spell-checking programs, such programs can highlight persons, companies, consumer products, and so forth. If the user clicks on the highlighted word, the client software will initiate a request to the appropriate Web service, and the user can receive a research report regarding the company; an encyclopedia entry for the individual; or a product review for the consumer device.

As bandwidth capacity becomes greater, Web services are likely to become increasingly "active." Based on the user's previous viewing patterns, for example, scanning software might select certain Web services to access and update automatically, without the user having to click on the highlighted word. In that way, the information is immediately present when the user clicks on the word, without any delay from accessing the Web service.

---

[21] John Markoff, *Microsoft is Ready to Supply a Phone in Every Computer*, N.Y. Times (June 12, 2001), at A1.

The services themselves are also likely to become increasingly more powerful. For example, if a user types in the name of a city, the scanning program might, based on the user's input and viewing habits, initiate a request to the user's online travel Web service. The Web service, in turn, would generate a trip itinerary with the airline, hotel, and car rental agency last used by the individual in that city. Once the user confirmed the reservations, the Web service would drop the relevant trip details into the user's calendaring program. Similarly, if the user identified the name of a company, the scanning program might generate a link to the user's online brokerage, whose Web service would generate not only the company's current stock price and relevant research information, but also how the company would fit into the user's existing portfolio in terms of relative volatility, industry weightings, and so forth. Once the user confirmed the purchase of the particular stock, the Web service would notify the user through the user's email account whenever there were earnings or other announcements from the company.

* * * *

In sum, a PC user in the near future might decide as a result of a real-time Internet conference with several colleagues to book an airplane flight to another city. After the user types in the city's name, the scanning engine might open links to two online travel agencies, one selected by the employer for business travel and the other preferred by the user for personal travel. One Web travel service might be accessed using the Web identity and authentication service chosen by the employer; the other might be accessed using the Web identity and authentication service chosen by

the user. After the user selects business versus personal, the travel agency might generate an itinerary based on the user's previous travel plans; purchase tickets and make hotel reservations using financial information provided by the authentication service; enter appropriate scheduling information in the user's calendaring program; and instantly notify the user in the event there are any delays in the scheduled flight.

Notably, the PC operating system -- the core of Microsoft's desktop monopoly -- is relatively peripheral to the provision of these services. Indeed, as discussed in Section III immediately below, the operating system's reduced significance in a world of distributed applications is amply evident in the forthcoming release of Microsoft's newest version of Windows, Windows XP. As Windows XP makes clear, the user interface for distributed applications principally will be the browser, not the Windows desktop. In a world where Microsoft faced competition to its browser, Microsoft's desktop monopoly accordingly might now be under siege. No such competition remains, however, and Microsoft consequently is pursuing a strategy whose focus is not simply maintaining its existing monopoly, but dramatically extending it -- a subject to which the analysis now turns.

III. FORTRESS MICROSOFT

In the past few months, Microsoft has announced a core set of Web services built on the .NET platform, code-named Hailstorm (March 2001), and it has released a beta version of Windows XP (due to be released October 25, 2001). With these product releases and announcements, the outlines of Microsoft's .NET strategy have become increasingly clear. Although some of the details of Microsoft's plan still may change, what is now apparent, as one senior industry analyst has

observed, is that "Microsoft has already put the wall around users." By the time Microsoft "puts the roof on," he concluded, "users will be inside Fortress Microsoft."[22]

If Microsoft's plan may be described as the building of Fortress Microsoft, Microsoft Passport, Microsoft's Web identity service, is the cornerstone of that plan. A monopoly in Web identity services will enable Microsoft to control the means by which users access distributed applications from the Internet. Reflecting its competitive significance, Microsoft has designed Windows XP so that Microsoft Passport is the exclusive Web identity service that it supports. To further accelerate adoption of Microsoft Passport, Microsoft has biased the user interface in Windows XP -- which principally has shifted from the operating system to the browser -- so that it systematically biases the display in favor of Microsoft sites and services that require Passport, such as Microsoft's instant messaging software (MSN Messenger) and its online services.

This section describes first how Windows XP forces adoption of Passport directly, and then turns to the means by which it indirectly forces adoption of Microsoft services that use Passport. This indirect forcing is accomplished principally through bias in the Windows XP user interface (which effectively has shifted from the operating system to Internet Explorer).

To the extent that Microsoft is found to have engaged in illegal conduct in connection with the case currently on appeal, Microsoft's ability to shift users to its Web identity service and distributed applications are an important way in which Microsoft will have benefited from its illegal conduct. Microsoft also will have benefited from its browser monopoly through the ubiquitous

---

[22] Maggie Holland, *Microsoft Users Face .NET Lock-In*, Computing (Mar. 22, 2001) (*quoting* IDC Vice President Dan Kuznetsky), *available at* 2001 WL 6038864.

distribution of the .NET program interface on which Microsoft's distributed applications are built. This section concludes by noting that, because of Microsoft's browser monopoly, Microsoft may already have won the race to own the platform on which distributed applications for consumers are built.

A. Laying the Cornerstone: Microsoft Passport

In order to ensure the universal adoption of Microsoft Passport, Microsoft executives indicated in their initial briefings to the media that Microsoft would take the bluntest approach possible -- that is, Microsoft would require users to sign onto Microsoft Passport whenever they accessed the Internet from Windows XP. In the beta version of Windows XP, Microsoft has not yet gone quite so far with respect to the visible part of Windows XP (the user interface), although it clearly anticipates doing so. As discussed in more detail later in this section, Microsoft already has done all of the development work that would be required. Microsoft in effect has developed two alternative user interfaces for Windows XP: a "plain" version of Internet Explorer 6.0, which does not require Microsoft Passport; and a version of Internet Explorer that has been "integrated" with MSN Messenger, called MSN Explorer, which *does* require Microsoft Passport.

It remains to be seen in the final version of Windows XP whether Microsoft will simply eliminate "plain" IE, and provide MSN Explorer as the principal user interface for Windows XP. "Under the hood," however, the decision already has been made. Indeed, Windows XP does not just directly promote Microsoft Passport -- it does so *exclusively*. Windows XP will support one, and only one, Web identity service: Passport.

There is no *technical* reason why Windows had to be configured this way. As two Gartner Group analysts recently observed, Windows could as easily have been configured to allow the user to select which Web identity and authentication service the user wished to employ. For example, such an alternative would have been easy to implement through a link to UDDI, an "Internet Yellow Pages" co-sponsored by Microsoft that provides users with a searchable registry of Web services. Rather than permit users to select their own identity service, however, Microsoft created an exclusive link to further its own ends:

> Microsoft regards Passport as a key leverage point and will use its own established platform dominance to drive exclusive usage. HailStorm does not require Windows platforms or Windows XP, but both Windows XP and Office XP will provide a level of convenience for users and will drive use of HailStorm services. Windows XP will use Passport exclusively for its identity service. . . . [F]or HailStorm to be as open as other .Net and Web service technologies such as UDDI and SOAP, Windows XP could use a UDDI look-up to allow selection from competing identity services. Microsoft has chosen not to do this.[23]

As discussed in more detail in Section IV, Microsoft's tie of its Passport Web service to Windows XP cannot be squared with the antitrust laws, even under Microsoft's own interpretation of them. The lack of legal justification, however, has not stopped Microsoft from using the full force of *all* of its monopolies to secure its ends. As the Gartner Group analysts note in their commentary, Microsoft has used Office as well as Windows and IE to drive exclusive use of Passport -- and Passport, in turn, is "the key leverage point" for Microsoft's domination of Web services (through Hailstorm) and the Internet as a whole (through .NET).

---

[23] David Smith and Chris LeTocq, *Commentary: Hailstorm's Consumer Focus*, Gartner Viewpoint on CNET News.com (Mar. 20, 2001), *available at* http://news.cnet.com/news/0-1003-201-5195835-0.html.

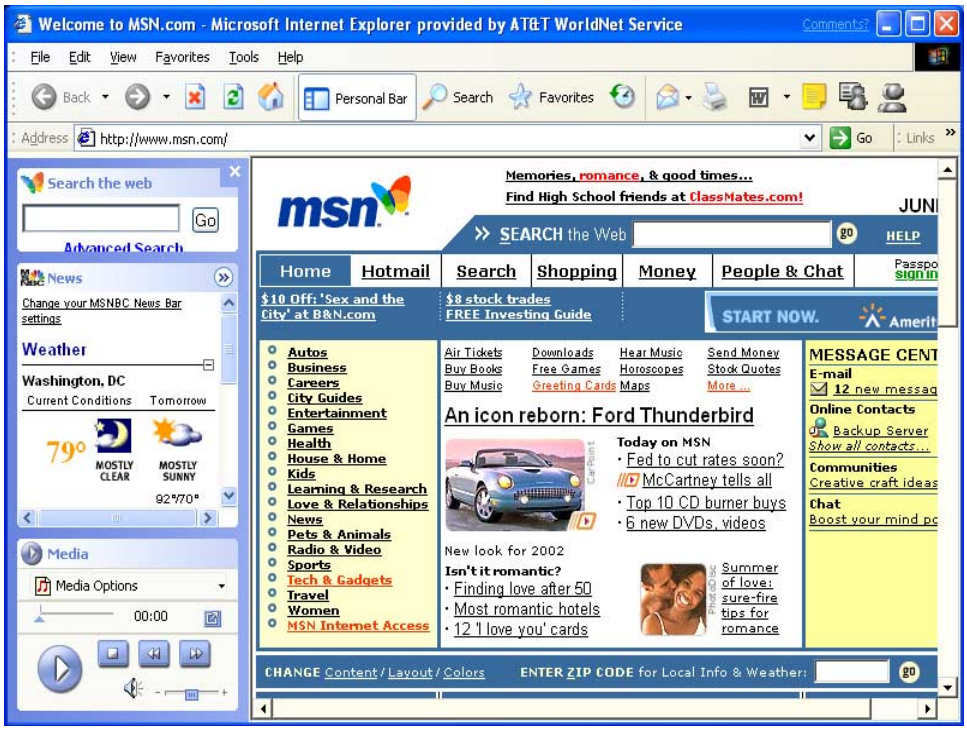
B. Raising the Walls: IE and MSN Explorer

One of the most striking features of the Windows XP user interface is the extent to which it reflects Microsoft's expectation that distributed applications and other online services soon will eclipse desktop applications as the software that users access most frequently. Indeed, in early betas of Windows XP, very little remains of the Windows user interface. Unlike Windows 95 and its successors, whose screen displays contained desktop icons, pop-up displays, tool bars, and other features designed to make as much functionality accessible as possible, most of that functionality was stripped away from the beta of Windows XP. Below is a copy of the screen display from the start menu of one of the recent builds of Windows XP:

Even if greater functionality ultimately is included in the final release of Windows XP, the beta releases show that Microsoft's focus has been on the displays of its two alternative browsers, IE 6.0 and MSN Explorer. As noted earlier, it is unclear whether Microsoft intends to offer both

browsers in its final release. In the beta versions of Windows XP, however, it is evident that IE and MSN Explorer constitute two separate models by which Microsoft can use Windows to extend its monopoly to Passport and related distributed applications.

IE 6.0. The "lesser" degree of forcing is reflected in the IE 6.0 interface, shown below.



This interface is reminiscent in layout to Microsoft's old Windows screen displays. The principal difference is that the bias in favor of Microsoft technologies is even more apparent. The IE "toolbar" on the left-hand side of the screen display, for example, features MSN Search, MSNBC News, and Windows Media Player. In the beta version of IE 6.0, the toolbar defaults to the open position, as shown in the picture above. While it can be closed manually after IE 6.0 starts, there is no readily apparent way for the user to alter the default "open" setting. Additional "services" can be added to the personal tool bar, such as Microsoft's Expedia travel service, MSN Calendar, and

Microsoft's Slate magazine. Other Microsoft applications, most notably MSN Messenger, are accessible from icons at the top of the screen display.

This screen display makes it difficult for a user to avoid invoking some Microsoft site or Web service that will require a Microsoft Passport. Running "under the hood," however, is arguably an even more powerful means of influencing consumer choice: a technology that Microsoft refers to as SmartTags.

The "scanning engine" that underlies SmartTags is not new technology: a more primitive version is present in Word 97, for example, as the technology that generates squiggly red lines to highlight potentially misspelled words. The scanning engine constantly compares the words being typed by the user with the words listed in Word's dictionary; if the word is not present in the dictionary, the program generates the red squiggly line. The same technology also generates a pop-up menu with the entire current date if the user begins typing in "July xx." By typing the Tab key, the user is able to avoid needing to type in the remainder of the date.

SmartTags takes that basic technology and applies it not merely to content created by the user, but to any Web page created by third parties that the user is viewing. SmartTags compares that content to a Microsoft directory and places purple squiggly lines under certain words or phrases, such as the names of people, companies, or products. If the user clicks on the word, Internet Explorer takes the user to a Web site with information about that matter. Microsoft has stated, for example, that company name links will "be available for all companies with a ticker symbol, [and] will guide users to Microsoft's MSN site, which provides information about companies listed on the

stock exchange."[24] Through SmartTags, Microsoft thus will effectively add its own layer of editorial content to information that the user receives from third parties on the Internet: the user will see not only the links that the Washington Post, for example, has chosen to include on its Web site, but the links that Microsoft creates through SmartTags as well.

Some of the broader policy issues raised by Microsoft's implementation of SmartTags are addressed later in Section V. For present purposes, however, what is noteworthy is that Microsoft has chosen to implement SmartTags in a way that persistently directs users to Microsoft's Web services. When the user types in a company name, for example, Microsoft chose not to allow the user to select from a menu of sites that provide stock price information, for example through a "UDDI" look-up. Microsoft also chose not to create links to the companies' own Web sites, which is what it did with the names of sports teams and universities. Instead, it simply creates a link that takes the user automatically from the word "IBM" to Microsoft's MSN MoneyCentral Web site.

As one article concluded regarding Microsoft's use of SmartTags, SmartTags "provide a natural segue to the company's planned set of .NET services."[25] Indeed, it seems likely that most users eventually will sign up for Microsoft Passport and simply use the omnipresent links that they will confront everywhere on the screen, both in the frame around the edges of the screen (through the IE tool bars) and throughout the content displayed on the screen (through SmartTags).

---

[24] "*Smart Tags" Link to Another Microsoft Controversy*, USA Today (June 8, 2001), *available at* http://www.usatoday.com/life/cyber/tech/2001-06-08-microsoft-smart-tags.htm (citing example provided by Microsoft lead group manager Greg Sullivan).

[25] *"Smart Tags" Link to Another Microsoft Controversy*, *supra.*

MSN Explorer. MSN Explorer takes the visible (IE screen display) and invisible (SmartTags) bias in IE, and goes one step further: it requires Microsoft Passport for initial log-on, and it automatically invokes Microsoft's instant messaging service. The MSN Explorer user interface is displayed below.

With MSN Explorer, after users enter their Microsoft Passport identification, they are logged onto the MSN Web site, which serves as the users' default home page. Users' email permanently defaults to Microsoft's Web-based email service, HotMail; the "travel" setting permanently defaults to Microsoft's travel service, Expedia; the "money" setting permanently defaults to Microsoft's MoneyCentral; the search setting permanently defaults to MSN Search; and the media player permanently defaults to Windows Media Player 8.0. None of these default settings may be changed. Using Microsoft Passport, moreover, all of the user's instant messaging communications (which now include text, videoconferencing, and telephony) will use Microsoft's instant messaging software.

In the world of MSN Explorer, in short, the user's Internet access will run through Microsoft, and all of the user's most essential Internet services will be provided by Microsoft. All of these services, moreover, will run on the .NET platform, which Microsoft has been able to make ubiquitous through its browser monopoly.

C. Putting on the Roof: .NET

A crucial reason for the durability of Microsoft's Windows monopoly has been that other developers must write their programs in a way that is compatible with Windows. Unless they do -- that is, unless they use the Windows "application program interfaces," or "APIs" -- users cannot get the application program to perform even the simplest tasks. Through its control of this Windows "program interface," Microsoft effectively stands between the application program and the user. Unless the application program conforms to Microsoft's APIs, Windows users simply will not be able to get the program to work.

.NET is important because it extends Microsoft's program interface (that is, its set of APIs) to provide the underpinnings necessary for distributed applications. As Microsoft explains on its Web site in a white paper entitled *An Introduction to Microsoft .NET*:

> Just as MS-DOS® and Windows® operating systems significantly changed computing, so will .NET. MS-DOS drove the acceptance of personal computers throughout businesses and homes; Windows elevated the graphical user interface to the preferred way of interacting with software, and the graphical user interface made personal computing mainstream. .NET is designed to make XML Web services the mainstream model for computing moving forward.[26]

---

[26] Microsoft white paper, *An Introduction to Microsoft .NET*, *available at* http://www.Microsoft.com/net/intro.asp.

At the heart of .NET is Microsoft's Common Language Runtime environment, or "CLR." Microsoft's CLR is a Java-like technology that allows developers to write one set of portable code for a virtual (or software-based) processor. This code will run on any device on which CLR has been deployed. Microsoft will include CLR with all of its most future versions of Windows, including Windows XP. CLR therefore is present on any machine containing those operating systems. Microsoft also has included critical CLR functionality in all copies of Internet Explorer,[27] including IE 6.0 and MSN Explorer. CLR will therefore become ubiquitous on client devices as a result of Microsoft's browser monopoly, even for those machines that do not run Windows.

CLR is modeled after, and would compete with, Sun Microsystem's Java technology, which also provides a program interface that could have been used for the development of distributed applications. In order for Java to compete as a platform for distributed applications, however, it would have to be deployed on the client machines that will be used to access these Web services. The success of Netscape's Web browser gave Java the opportunity to achieve such client-side distribution, because Java was distributed with the Netscape browser.

Microsoft's success in monopolizing the browser market, however, has had the effect of blocking Java's penetration of the market, while accelerating the ubiquity of CLR. Internet Explorer is not, of course, Microsoft's only means of ensuring the ubiquity of CLR. Microsoft's distribution of CLR with Windows also gives it the ability to reach the 93% or so of PC users who use Windows.

---

[27] *See, e.g.*, *Runtime Hosts*, Microsoft .NET Framework Developer's Guide, *available at* http://msdn.microsoft.com/library/dotnet/cpguidnf/cpconruntimehosts.htm (2001).

Since something like 72% of adult Americans own PCs, Microsoft also has the ability to reach roughly 68% of the population through its Windows monopoly.

The issue with browsers, however, was not whether Microsoft would be able effectively to penetrate the market with CLR, but whether a competing runtime environment would be present on users' machines as well. With the marginalization of the Netscape browser, CLR is likely to be the only runtime environment for distributed applications present on most client devices. Combined with the sole support for Microsoft Passport in Windows XP, and the display biases and ties in IE and MSN Explorer, the description of consumers residing in "Fortress Microsoft" appears only too likely to turn into another Microsoft *fait accompli*.

IV. COSTS AND CONSEQUENCES

The use of Microsoft Passport as the exclusive identity service for Windows XP, the use of SmartTags, and the bolting of other services and applications into Windows XP, raise at least three separate policy issues. First, Microsoft's forthcoming release of Windows XP appears to constitute a new violation of Section 2 of the Sherman Act, which prohibits monopolization and attempted monopolization. Second, Microsoft Passport and Microsoft's related Hailstorm Web services raise very serious privacy and security issues, given Microsoft's statements regarding how it will collect and use the information that it aggregates through these services. Finally, Microsoft's potential monopoly raises more general policy issues regarding the consequences of allowing one company to control the means by which users access the Internet.

A. Sherman Act Issues

The pending decision by the Court of Appeals in *United States v. Microsoft* is likely to address the standard that should be used to determine the circumstances under which Microsoft can bolt other Microsoft applications and services to its Windows monopoly product. What is striking about Windows XP, however, is that Microsoft appears to have designed this forthcoming release -- the most significant new release of Windows since Windows 95 -- in a way that disregards even the limitations that Microsoft's own attorneys have acknowledged during the course of the appeal. Nowhere does this contradiction seem more apparent than Microsoft's bolting of Microsoft Passport as the exclusive identity service supported by Windows XP.

To begin with, under Section 2 of the Sherman Act, a company with monopoly power cannot use that monopoly power "to foreclose competition, to gain a competitive advantage, or to destroy a competitor." *Eastman Kodak Co. v. Image Technical Services, Inc.*, 504 U.S. 451, 482-83 (1992); *see also id.* at 498 (Scalia, J., dissenting) (The antitrust laws do not permit a monopolist "to project its monopoly power into another market, *i.e.*, to 'exploit his dominant position in one market to expand his empire into the next'") (*citation omitted*). Although Microsoft contests it, most observers believe that it is clear that Microsoft does in fact exercise monopoly power in Windows. The question accordingly is whether it has used that Windows monopoly improperly either to maintain that monopoly or to "exploit [its] dominant position in one market to expand [its] empire into the next." *Id.*

On appeal in *United States v. Microsoft*, Microsoft has argued that it did not violate the antitrust laws because an exception should be created for "integrated" products. In invoking this "integration" defense, Microsoft relies heavily on *United States v. Microsoft Corp.*, 147 F.3d 935 (D.C. Cir. 1998), a decision that did not directly address the issue whether Microsoft had violated the

Sherman Act, but rather considered whether Microsoft had violated a specific provision in the parties' 1994 consent decree.[28] In that case, the Court of Appeals focused on two factors to determine whether a product was "integrated" as that term was used in the consent decree. First, "the combination offered by the manufacturer must be different from what the purchaser could create from the separate products on his own." Second, the combination "must also be better in some respect; there should be some technological value to integration. Manufacturers can stick products together in ways that purchasers cannot without the link serving any purpose but an anticompetitive one." 147 F.3d at 948.

The Court of Appeals emphasized that its standard imposed real limits on the meaning of an "integrated" product. It concluded, for example, that its interpretation was consistent with the Supreme Court's decision in *Eastman Kodak*, in which the Supreme Court had found parts and service to constitute separate products because sufficient consumer demand existed to make separate demand efficient. *Id.* at 950. To illustrate these limits, the Court of Appeals hypothesized what would happen Microsoft had bundled a computer mouse with the operating system. The Court stated: "If for example, Microsoft tried to bundle its mouse with the operating system, it would have to show that the mouse/operating system package worked better if combined by Microsoft than it

---

[28] In interpreting the decree, the Court looked in part to "tying" law. A tying arrangement 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." *Eastman Kodak*, 504 U.S. at 461. In the context of Section 1 of the Sherman Act, which prohibits contracts in restraint of trade, a tying arrangement is illegal if the seller has "appreciable market power" and the arrangement affects a substantial volume of commerce in the tied market. Under Section 2 of the Sherman Act, which prohibits monopolization and attempted monopolization, a tying arrangement is illegal if the seller has monopoly power and it has used that power "to foreclose competition, to gain a competitive advantage, or to destroy a competitor." *Id.* at 462, 482-83.

would if combined by OEMs." The Court then observed: "Problems seem unlikely to arise with peripherals, because their physical existence makes it easier to identify the act of combination." Under such circumstances, a plausible claim of integration is "unlikely":

> It seems unlikely that a plausible claim could be made that a mouse and an operating system were integrated in the sense that neither could be said to exist separately. An operating system used with a different mouse does not seem like a different product. But Windows 95 without IE's code will not boot, and adding a rival browser will not fix this.[29]

If Microsoft defends its bolting of Web services (including Passport) to Windows XP on "integration" grounds, the Court's analysis condemns Microsoft here. To begin with, these Web services are physically distinct from Windows: they reside on servers in Redmond, Washington (or wherever Microsoft has its server farm), not on the user's local machine. Moreover, they are quite literally "services," which, as the Court of Appeals noted, the Supreme Court has recognized as products separate from "parts." Indeed, unlike the copier service and parts involved in *Eastman Kodak*, there is nothing about these Web services that is specifically directed to the PC or the PC operating system. Microsoft executive Robert Hess made that point quite forcefully, stating that the services were designed to run on "any device, any service, anywhere on the planet," regardless of "whether it's a cell phone, a PDA, a PC or whatever kind of device it is," and regardless of whether it is running Windows or Linux.[30]

---

[29] 147 F.3d at 948 n.11.

[30] *Web Services, an Interview with Robert Hess* (Mar. 19, 2001), *available at* www.microsoft.com/business/vision/hess_on_web_services.asp.

Microsoft's bolting of Passport to Windows is particularly striking because it constitutes the very antithesis of "integration" under the Court of Appeals' standard: the products are not simply unrelated; rather, the absence of any link is essential to the core functionality of an identity service. That is because the whole purpose of authentication is to obtain third-party verification of the user's identity from a source *unrelated* to the local machine. The more involved the user's local operating system in the authentication service, the more inferior (indeed, useless) the service.

It is difficult to envision what other defense Microsoft might have for Passport exclusivity. The number of Passport users already dwarfs any other identity service: according to Microsoft, there are already *160 million* Passport accounts.[31] Microsoft therefore cannot claim that bolting Passport to Windows is necessary to jump-start a new service against an entrenched competitor. Nor can Microsoft claim that it would impose undue burden on the company to allow consumers to select their own identity service. Indeed, the purpose of using XML in its Web services, as Microsoft readily acknowledges, is to allow users to obtain easy access to multiple XML Web services from any device. Microsoft's Passport exclusivity affirmatively *impairs* this functionality by seeking to limit access to an important class of XML Web services (i.e., identity/authentication services) on devices running Windows XP.

Apart from its Web services, Microsoft's bolting of other distributed applications, including IM, to Windows XP, also would seem likely to violate the Sherman Act, regardless of the standard adopted by the Court of Appeals in its pending decision. Indeed, the only way that Microsoft

---

[31] *Remarks of Microsoft Group Vice President Bob Muglia*, Hailstorm Announcement (Mar. 19, 2001), *available at* http://www.microsoft.com/billgates/speeches/2001/03-19hailstorm.asp.

apparently defends the ties and links in Windows XP is on the ground that the entire Internet effectively can be "integrated" as part of Windows. That is what Microsoft's executives, if not its lawyers, readily acknowledge:

> The role that the Windows platform played in the past and the role it plays in the future is absolutely the same. Today we have a world of applications and Web sites, and we think of those as two different worlds. With .NET, they become one. Some Web sites will be richer applications than others, but essentially everything that was an application becomes a Web site with application services. Windows 2000 [Windows XP] is the cornerstone of the .NET vision. . .[32]

Under the rationale that all applications are now Web sites and all Web sites are now applications, Microsoft proclaims that they can all be integrated into the Windows platform and "become one." It remains to be seen what enforcement position the United States will take with respect to this striking claim. Even if none of Microsoft's conduct is determined to violate the antitrust laws, however, the prospect of Microsoft attaining monopoly power in Web services and other distributed applications raises serious policy concerns on several levels.

B. Privacy Issues Raised by Passport and Hailstorm

As noted earlier in this section, Microsoft claims already to have 160 million Passport accounts.[33] Passports are required in order to use Microsoft's MSN online service; its MSN Messenger instant messaging application; and its Hotmail Web-based email service. There are also

---

[32] Paul Thurrott, *Microsoft Responds: Win2K is the Cornerstone of .NET*, Windows 2000 Magazine (Nov. 7, 2000) **(**remarks of Microsoft marketing director Mark Perry), *available at* http://www.win2000mag.com/Articles/Index.cfm?ArticleID=16068.

a large number of Passport sites, including CostCo, Buy.com, Radio Shack, Office Depot, Godiva, Victoria Secret, and many Microsoft sites.[34] Microsoft accordingly already has collected what probably amounts to *trillions* of bytes of information about users, even before the launch of Windows XP. The imminent launch of Windows XP (currently scheduled for October 2001), however, and the prospect of Microsoft obtaining a monopoly in the "killer" distributed applications, including Web services, serves to underscore the need to consider the privacy and security issues raised by Microsoft's plans.

To begin with, and as a point of comparison, it is useful to consider how user information currently is handled by online sites. Three features that facilitate the protection of privacy with respect to the present regime are particularly worth noting. First, information that Web sites collect today typically is not identifiable to any person: an online bookstore might know that user "BillSmith3" has a preference for biographies and jazz, but the information that it collects generally is not identifiable to a particular human being Bill Smith living in Boise, Idaho. Second, the information may be used by the online book store in exchanges with BillSmith3, but is not shared with other Web sites. Significant controversy has arisen in the past when companies have proposed to share information across multiple sites. Third, the information is maintained on a decentralized basis: there is no central repository that hackers or others can attempt to access.

---

[33] *See Hailstorm Announcement: Remarks by Bill Gates*, Microsoft (March 19, 2001) <http://www.microsoft.com/billgates/speeches/2001/03-19hailstorm.asp> (remarks of Microsoft Vice President Bob Muglia).

[34] *See Passport – Directory of Sites*, Microsoft (last visited June 18, 2001) <http://www.passport.com/Directory/Default.asp?PPDir=C&lc=1033> (listing current Passport-enabled sites).

Microsoft's plans with respect to Passport propose precisely the opposite model: Microsoft proposes to collect personally identifiable information; to obtain as much of this information as possible; to share this information with other Web site vendors; and to maintain a centralized database under Microsoft's control. Each of these points is considered in turn.

First, Microsoft unquestionably seeks to collect as much personally identifiable information as possible through Passport and the Web services that build upon it. With Passport, Microsoft stores the user's name, password, and other information necessary for user identification and authentication. Microsoft's Web services then build upon this digital Passport identity by aggregating additional user information, such as the user's credit card numbers, contact list, and calendar. A list of Microsoft's Hailstorm Web services includes:

My Address (electronic and geographic address)

MyProfile (name, nickname, special dates, picture)

MyContacts (electronic relationships and address book)

MyNotifications (notification subscription, management and routing)

MyInbox (inbox items from email, voicemail)

MyCalendar (time and task management)

MyDocuments (document storage)

MyApplicationSettings (favorite Web addresses and other Web identifiers)

MyWallet (receipts, payment instruments, other transaction records)

MyUsage (usage report for these services)

MyLocation (electronic and geographical location and rendezvous)[35]

Second, Microsoft intends to share this information with other Web site providers. This sharing will occur in two ways -- one of which Microsoft advertises, the other it does not. To begin with, Microsoft specifically promotes Passport and its related Web services on the ground that they "manage[s] such basic elements of a user's digital experience as a calendar, location, and profile information. Any solution using Hailstorm can take advantage of these elements, saving the user from having to re-enter and redundantly store this information and saving every developer from having to create a unique system for these basic capabilities."[36] To illustrate these advantages, Microsoft gives an example of a traveler using an online travel service:

> Hailstorm will help enable the travel service to automatically process the individual's payment information. If traveling on business, a user's affiliation with their company's Hailstorm group identity makes it possible for the travel service to automatically show only the choices that meet the traveler's individual preferences and which adhere to the company's travel policies. Once the user has chosen the flight, the travel service can use Hailstorm -- with the traveler's permission -- to automatically schedule the itinerary onto the specific calendaring service he or she uses. Through Hailstorm, live flight information can be shared with whomever the traveler designates...[37]

---

[35] *See Building User-Centric Experiences: An Introduction to Microsoft HailStorm*, Microsoft (March 2001), *available at* http://www.microsoft.com/net/hailstorm.asp.

[36] *Id.*

[37] *Microsoft Announces "HailStorm," a New Set of XML Web Services Designed to Give Users Greater Control*, Microsoft (March 19, 2001), *available at* http://www.microsoft.com/presspass/features/2001/mar01/03-19hailstorm.asp.

In this example, Microsoft sends the online travel service credit card information, calendaring information, and contact information about the user. Microsoft emphasizes that the information shared by Microsoft with the online travel service is "with the traveler's permission," but what it does not stress is that any information collected *by the online travel service* can be (and likely will be) automatically shared with Microsoft, *without* the user's permission. Information that the user provides to any Passport Web site is stored by that Web site in a "cookie" and delivered to Microsoft. By the end of the Passport user's online session, Microsoft knows every Passport-enabled Web site that the user has visited. With respect to the information collected by Passport sites and delivered to Microsoft, Microsoft's policy simply is *caveat emptor*:

> Passport uses cookies whenever you sign in to a participating Passport site. The Passport site stores your member name, the time you signed in, and your profile information in a secure, encrypted cookie on your hard disk. The cookie contains information that you chose to provide to that Web site. You are in charge of deciding what information sites know about you.[38]

Third, Microsoft not only intends to collect and share voluminous amounts of personally identifiable data, but it has reserved the right to do whatever it wishes to with the information. Until a few months ago, when it attracted a wave of adverse publicity, Microsoft's policy in this regard was particularly brazen. Although written in "legalese," it warrants careful consideration:

> [By] inputting data . . . or engaging in any other form of communication with or through the Passport Web Site [or any of its associated services], [you grant Microsoft the right to] use, modify, copy, distribute, transmit, publicly perform, reproduce, publish, sublicense, create derivative works from, transfer or sell any such communication [and] exploit any proprietary rights in such communication,

---

[38] *Microsoft Passport: Privacy Statement*, Microsoft (updated July 2000), *available at* <http://www.passport.com/Consumer/PrivacyPolicy.asp?PPlcid=1033>.

> including but not limited to rights under copyright, trademark, service mark or patent law.

In the wake of the adverse publicity attracted by this provision, Microsoft modified its policy, stating that "the Passport.com terms of use that had been in effect . . . were, unfortunately, woefully out of date. It was obviously an unfortunate error and oversight on our part."[39] Microsoft did not explain why this "out of date" policy was appropriate previously, during a period in which Microsoft gained 160 million Passport accounts. Moreover, Microsoft still has not imposed any significant limits on its ability to use and share information. For example, Microsoft still does not give users the ability to limit the flow of cookies from Passport Web sites to Microsoft, and its privacy policy imposes no limits on Microsoft's ability to utilize or disclose that information.

Microsoft also reserves the right unilaterally to change its mind. According to Microsoft policy, users who continue to use Passport after Microsoft changes the privacy policy on its Web site have consented to any such changes:

> Microsoft reserves the right to change the terms, conditions, and notices under which the Passport Web Site and Passport Services are offered. You are responsible for regularly reviewing these terms and conditions. Continued use of the Passport Web Site or Passport Services after any such changes shall constitute your consent to such changes.[40]

---

[39] Monty Phan, *Microsoft Revises 'Passport' / But use of Web users' info remains an issue*, Newsday, April 6, 2001, A57, 2001 WL 9225261 (quoting Microsoft Spokesman Tom Pilla).

[40] *Microsoft Passport: Terms of Use*, Microsoft (revised April 4, 2001), *available at* http://www.passport.com/Consumer/TermsOfUse.asp?lc=1033.

And although users are cautioned that continued use of Passport constitutes their implied consent, they are not informed that Microsoft limits their ability to exit the system. A recent request by a Passport user asking to delete the user's Passport account received the following response:

> Hello Alex,
>
> *Thank you for writing to Microsoft Passport. To delete your Passport account, discontinue using the Passport service. After 12 months of inactivity, our system will automatically delete your account*.
>
> You may register for a new Passport account at any time. Microsoft Passport has comprehensive online help available to you. For your information on Passport features, functions, and issues, click the "help" button on the horizontal navigation bar or go to [link omitted]. Thank you for using Microsoft Passport. If you have further questions, please contact us again.
>
> Sincerely,
>
> Roberto Antonio, Microsoft Passport Customer Support Representative

Fourth, Microsoft will aggregate all of the personalized information that it collects into a centralized database that is likely to have far more data about users than any existing database today. In so doing, Microsoft will create for hackers a target of unique value (and potential for mischief). The potential seriousness of this problem is perhaps best highlighted by the fact that less than a year ago, the *New York Times* reported under the headline "Microsoft Says Online Break-In Lasted 6 Weeks": "Unidentified intruders had access to Microsoft computers for about six weeks and were able to view some of the source code -- a programmer's basic instructions -- for a future software product, the company said yesterday."[41]

---

[41] John Markoff and John Schwartz, *Microsoft Says Online Break-In Lasted Six Weeks*, New York Times (Oct. 28, 2000).

There is no doubt that Microsoft protects its source code, the company's "crown jewels," with the best security that it can devise. That hackers nonetheless were able to enter the Microsoft network repeatedly over a period of many weeks and access such source code is an important yardstick by which to measure the security risks posed by the vast user database that Microsoft is constructing.[42] Indeed, Microsoft's vast centralized database arguably creates precisely the weakness from a privacy and security perspective that the Internet was designed to prevent from a defense perspective: that is, the vulnerability created by the centralized management and control of data on the network.

In sum, in place of the current system of decentralized aggregation of information, not personally identifiable to the user, and not widely shared among Web sites, Microsoft is building a centralized database that will collect detailed, personally identifiable information about millions of users from a wide variety of Web sites, with no effective restrictions on its right to use that information. At present, it appears unlikely that users will be able to select this system from among

---

[42] This hacker attack was not the only security breach that Microsoft has experienced in the last year. *See, e.g.*, Robert Lemos, *Microsoft Security Flaw Threatens Web*, CNET News.com (June 18, 2001) ("Microsoft said Monday that a 'serious vulnerability' in its flagship Web server software used by computers running more than 6 million sites could allow hackers and online vandals to take control of the computers"); Robert Lemos, *Microsoft "Incredibly Sorry" About Goofed Fix*, CNET News.com (June 13, 2001) ("Microsoft contritely acknowledged Wednesday that its second attempt to fix an Exchange security hole went awry. Rather than fix the problem--and the security hole--the company's second attempt at a software patch included a catastrophic bug that caused many servers to hang."); Robert Lemos, *Microsoft Races to Plug Web Security Hole*, CNET News.com (May 1, 2001) (Microsoft announced a serious security hole Tuesday in its flagship Web server software and raced to convince system administrators to patch their Web servers before online vandals compromise their systems. . . . 'It is a serious vulnerability,' said Scott Culp, security product manager for the software giant.); Chris Gaither, *Microsoft Sites Shut, This Time in Network Attack,* New York Times (Jan. 26, 2001) (Business Section).

competitive alternatives, free from the exertion of Microsoft's monopoly power; and there appear to be few safeguards in place to prevent the abuse and misuse of this information.

C. Microsoft's Control of Internet Content

Microsoft's control over the means by which users access the Internet raises issues not only because of the information that it will be able to collect and use, but also because of its resulting ability to exercise control over online content. Microsoft's SmartTags, which it has built into both its monopoly browser and its monopoly Office suite, vividly demonstrates how Microsoft can exercise such control.

As described previously, the SmartTags "scanner" will look at the content the viewer is reviewing (a Web page, a word-processed document) and apply a set of rules in an effort to find matches in that content. For example, it might apply a rule that reviews the page for the names of publicly traded corporations. Once a match has been found, it will take a predetermined action in accordance with that rule, such as putting a purple squiggly line under the name of the corporation. If the user clicks on the name, it links to a Web site containing the corporation's stock price.

As technology that runs on virtually every browser and virtually every productivity application, SmartTags gives Microsoft unparalleled opportunity to "edit" the content of other Web sites to suit its own purposes. By placing the SmartTags scanner in Internet Explorer, Microsoft in effect interposes itself between content creators and online users.

There are any number of ways in which Microsoft can use this technology to its benefit. To begin with, it enables Microsoft to free-ride on third-party content by obtaining advertising for free. SmartTags highlights terms found in third parties' content that are related to goods or services that

Microsoft wishes to sell. Microsoft then inserts links to its own Web sites offering those goods and services. Through its monopoly control of the browser, Microsoft thus is able to overlay its own free advertising onto another company's Web site.

Microsoft can be expected not only to use SmartTags for its own advertising, but also potentially to sell such advertising links to others. For example, every time the word "newspaper" appears in content that the user is viewing, Microsoft might sell to the highest bidder the right to appear on the resulting pop-up window. Because Microsoft is a browser monopolist -- that is, essentially all Web content is viewed via its browser -- SmartTags would instantly transform Microsoft into the most powerful online advertising agency. No other company could match Microsoft's offer: "Pay us and we'll put links to you on every Web site in the world that contains the terms you specify. No need to obtain permission any longer from individual Web sites, because we (Microsoft) have control over the portal that everyone uses to view those sites, and we will insert a link to you on the Web pages that the user sees."

There is no reason Microsoft would have to limit itself to editing third-party content for advertising purposes. Today, Microsoft uses SmartTags simply to *add* content to third-party sites. But precisely the same technology would enable Microsoft to implement rules that would cause the scanner to replace existing links to other's content with links to its own. A link to cnn.com inserted by the third-party Web site, for example, could be replaced with a link to msnbc.com. Other links might be deleted altogether. It would be for Microsoft to decide, for example, whether and how to link to "antitrust."

Finally, there is no reason why Microsoft's links would have to be limited to Web site content. Microsoft as easily could apply SmartTags to insert advertising or other links into content that the user creates. For example, the computer user's instant message or email might be delivered with links to Microsoft products or services.

Microsoft recently has claimed that the final release of Windows XP will be delivered with SmartTags turned off by default. There is no guarantee, however, that this default will remain "off" in the future, particularly in the absence of any competition in the means by which users access online content. Microsoft's other solution -- it claims that it will enable third-party sites to block SmartTags from appearing on their Web pages -- perversely imposes the burden on others to stop Microsoft from imposing unwanted bias.

Technology reviewers have rightly expressed alarm at the implications of SmartTags in a world where Microsoft enjoys a browser monopoly. As Walter Mossberg of the *Wall Street Journal* observed: "[I]f the feature is so benign, why is Microsoft hiding it and offering sites a way to block it?" He continued, "Microsoft's Internet Explorer SmartTags are something new and dangerous. . . . Microsoft as a perfect right to sell services. But by using its dominant software to do so, it will be tilting the playing field and threatening editorial integrity."[43]

V. POTENTIAL REMEDIES

---

[43] Walter Mossberg, *Dangerous Detours: Windows XP May Add its Links to Others' Sites*, Wall Street Journal, at B1 (June 7, 2001).

Microsoft's conduct raises serious policy issues that are not easy to resolve. Prior experience suggests that behavioral remedies, even if they could be imposed in detailed terms, would be ineffective in imposing any significant constraint on Microsoft's ability to use its existing monopoly power to obtain a monopoly in distributed applications. In the event that Microsoft is found to have engaged in illegal conduct under Section 2 in the pending browser case, a prompt structural remedy, in which Microsoft's Office and Windows monopolies are separated, might create a viable competitor before consumer "lock in" can take effect. A delay in the imposition of an effective remedy, however, is likely to delay the restoration of competition to the market by many years, if not decades.

A. Behavioral Remedies: the 1994 Consent Decree

The Justice Department's experience with the 1994 consent decree against Microsoft shows how difficult it can be to put in place an effective behavioral remedy. In 1994, the United States concluded that Microsoft had illegally maintained its operating system monopoly in violation of Section 2 of the Sherman Act by entering to a series of "per processor" licenses with the major computer manufacturers between 1988 and 1994. From the United States' perspective, therefore, the Windows monopoly that Microsoft currently enjoys (of which Windows XP will be the latest release) was secured in part through illegal conduct carried out over a period of several years.

To remedy this illegal conduct, the Justice Department entered into a consent decree with Microsoft that not only prohibited the specific illegal acts in which it believed Microsoft had engaged, but also included a series of "prophylactic" measures designed to ensure that Microsoft did not "attempt to extend or protect its monopoly" in some other way. One of these provisions, Section

IV(E), provided that Microsoft was prohibited from conditioning the licensing of the operating system on the licensing of some other product. The Justice Department explained:

> Section IV(E) prohibits Microsoft from expressly or impliedly conditioning its licenses of operating systems on the licensing, purchase, use or distribution not only of other covered products, but also any other Microsoft product, or non-Microsoft product. Without these provisions Microsoft could force OEMs to purchase covered products and thus accomplish anticompetitive effects similar to those achieved through its unlawful licensing practices, or attempt to extend or protect its monopoly in any covered product by conditioning its licenses on the licensing, purchase or use of other products.[44]

Three aspects of events subsequent to the entry of the 1994 decree warrant consideration. First, to the extent that the Justice Department had any expectation that the 1994 action would result in increased competition in the operating systems market, that expectation has been disappointed. In the years since the consent decree was entered, competition in desktop operating systems has declined significantly. In 1993, according to the Justice Department, IBM's market share of the PC operating systems market was 17%; Novell's was 3%; and Unix systems were 1%.[45] Apple was excluded from the market as the Justice Department defined it, but assuming its market share (of all desktop operating systems) was at least 5%, the market share of Microsoft's competitors was greater than 25%. Today, by contrast, Microsoft's competitors have a combined 7% market share: 4% for

---

[44] Competitive Impact Statement, *United States v. Microsoft*, No. 94-1564, at 11 (D.D.C. July 15, 1994), *available at* http://www.usdoj.gov/atr/cases/f0000/0045.htm.

[45] *Id.* at 4 n.2 (Microsoft 1993 PC desktop operating system market share was 79%; IBM share (PC-DOS and OS/2) was 17%; Novell was 3%; and Unix systems were 1%).

Apple, 1% for Linux, and 2% for "other."[46] Since the time the 1994 decree went into effect, therefore, the market share of Microsoft's competitors has dropped from 25% to 7% -- that is, from roughly one computer in four, to less than one computer in twelve.

Second, behavioral proscriptions such as those in the 1994 decree can have important limitations. In 1997, the Justice Department concluded not only that Microsoft had breached the consent decree when it bundled Internet Explorer with Windows 95, but that the issue was clear enough that it warranted the filing of a petition for contempt and motion for preliminary injunction. The district court agreed and entered a preliminary injunction. The Court of Appeals reversed, with a 2-1 split among the appellate panel as to the meaning of language in Section IV(E) stating that the provision "in and of itself shall not be construed to prohibit Microsoft from developing integrated products."

The Justice Department's action in 1997 shows that the agency believed that it had obtained an order that would prohibit the conduct in which Microsoft was engaged. It was only several years *after* the consent decree that the Department learned that the order not only was ambiguous (indeed, the appellate majority did not accept either the Justice Department's or Microsoft's interpretation, but came up with a third interpretation of its own), but that it did not reach conduct that the Justice Department thought it had proscribed. Moreover, although the Justice Department filed a new, separate action even before the Court of Appeals' decision, in hindsight we know that its opportunity

---

[46] International Data Corporation, *Client Operating Environments: 2000 Year in Review* (Feb. 2001). Commenting that "the strong are getting stronger," IDC noted that Microsoft's market share actually had increased 3%, from 89% to 92%, in 2000. *See* IDC Press Release, *Microsoft Strengthens Its Grip, Narrowing the Window of Opportunity for Other Operating Environments* (Feb. 28, 2001), *available at* http://www.idc.com/software/press/PR/SW022801pr.stm.

to obtain sufficiently prompt relief had been lost for good: a browser market that was competitive in 1997, when the contempt action was filed, had been monopolized by Microsoft long before the appeal in the Justice Department's subsequent action had been resolved.

Wholly apart from the question whether Microsoft's conduct with respect to Internet Explorer in fact violated the antitrust laws, the consent decree was ineffective as a means of preventing such conduct. The Justice Department attempted in 1994 to anticipate all of the different ways in which Microsoft might "attempt to extend or protect" its Windows monopoly. With Microsoft's bundling of Internet Explorer, it came very close -- close enough to think it had hit the bull's eye. In fact, however, as is so often the case with written instruments, the agency's understanding proved to be insufficiently set forth in the agreement's terms. The decree's "prophylactic" terms proved wholly useless in preventing what the Justice Department viewed as precisely the conduct that it sought to prohibit: Microsoft's maintenance and extension of its Windows monopoly through the bundling of other products (such as Internet Explorer).

Microsoft's conduct subsequent to the Court of Appeals' contempt decision raises a final point relevant in considering the efficacy of behavioral remedies, particularly with respect to Microsoft. During the course of litigation over the consent decree, the Justice Department claimed that Microsoft representatives had told the agency that Microsoft was free to bundle "a ham sandwich" with Windows if it chose to do so.[47] Microsoft strenuously argued that its statement had been taken out of context. Even assuming that to be the case, however, only a "ham sandwich"

---

[47] Reply Brief of Petitioner United States of America, *United States v. Microsoft*, No. 94-1564 (Nov. 20, 1997), at 5.

rationale appears sufficient to explain all of the software that Microsoft subsequently has bundled with Windows.

Windows 98 SE (Second Edition), for example, released in May 1999, bundled in FrontPage Express (Microsoft's Web page editor), WebTV for Windows (the client software for Microsoft's interactive television service), Outlook Express (an e-mail client); Microsoft NetMeeting (Internet conferencing client software); and Media Player (Microsoft's client software for streaming media). Windows Me (Millenium Edition), released in June 2000, similarly bundled in Movie Maker (Microsoft's video editing software) and MSN Messenger (Microsoft's instant messaging service), along with Outlook Express, NetMeeting, and Media Player. As discussed in more detail in Section II, the Windows XP beta takes this pattern even further, with Movie Maker, MSN Messenger, Outlook Express, and Media Player (among other programs) all bolted to Windows, together with exclusive support or hardwired links to Passport, MSN Search, MSNBC news, and a long list of other Microsoft sites and services.

If the consent decree permits the bundling of all of these products, sites and services, it plainly has no real substance. FrontPage Express and Movie Maker, for example, are editing tools, not different in function from word processing. If these programs properly can be bundled with Windows, so too could most if not all of the programs that in 1994 were part of Microsoft Office -- a result that the Justice Department almost certainly did not intend. Moreover, it seems unlikely that all of these products properly could be viewed as "integrated" with Windows under the standard adopted by the Court of Appeals. The WebTV television service whose client was bundled with Windows 98 SE, and the Passport identity service bolted to Windows XP, for example, would seem to be examples of services for which the PC is simply (to use Mr. Gates' terminology) the

"endpoint," and no more "integrated" with the operating system than the operating system is integrated with a computer mouse.

Even assuming that Microsoft is correct, however, that all of these products and services can be bundled with Windows, notwithstanding Section IV(E) -- and, hence, that the provision effectively is meaningless, because the "integration" exception swallows the "no bundling" rule -- Microsoft's conduct underscores a third point regarding behavioral remedies of the type set forth in the consent decree. Microsoft has proved willing over the past six years to press to the limit (and, in the Justice Department's view, sometimes beyond it) with respect to the meaning of prohibitions that otherwise might limit its behavior. To be effective, therefore, behavioral remedies would have to be comprehensive, highly detailed, and unambiguous; and, even so, litigation might be required to resolve provisions that proved to have serious bite.

In short, behavioral remedies appear likely to require prolonged government involvement that will either be intrusive or ineffective. The existing behavioral remedies have proven ineffective at maintaining or restoring competition (as to both Windows and Internet Explorer); they have proven ineffective as a "prophylactic" in limiting Microsoft's bundling with Windows (as witness Microsoft's bundling with Windows SE, Me, and XP); and they have proven ineffective at avoiding the necessity for further government enforcement action (as witness the contempt and browser actions). Paradoxically, structural remedies, far from requiring *greater* government involvement, may require *lesser* government intervention over time. How one such remedy might work is the subject of the following section.

B. Structural Remedies: Separating Windows and Office

In the event Microsoft is found not to have violated either Section 1 or Section 2 of the Sherman Act in the presently pending action, the issue of structural relief obviously is moot. In the event that Microsoft *is* found to have violated the antitrust laws, however, either in the maintenance of its Windows monopoly, or in attempting to obtain a browser monopoly, structural relief appears potentially to be both warranted and to hold out the prospect of effective relief.

To begin with, structural relief would appear to be appropriate in view of the scope of the monopoly which Microsoft thereby secured. Some sense of this scale may be gained by considering just how dominant is Microsoft's market position is relative to its only browser competitor, AOL/Netscape. AOL has used Internet Explorer in its online network, in large part to secure an icon for its online service on the Windows desktop.[48] A market research firm recently calculated that if AOL successfully switched 100% of its online user base from IE to its own browser (which seems like a relatively aggressive assumption), it would effect a swing of only 6.5% in browser market share: that is, Microsoft's browser dominance would change from 86.5% to 80%, while AOL's market share would rise from 13% to 19.5%.[49] At best, therefore, AOL could achieve browser

---

[48] *See, e.g.*, *United States v. Microsoft*, 84 F. Supp. 2d 9, 84 (D.D.C. 1999) (findings of fact) (Quoting AOL internal memorandum stating that "In exchange for using IE as our primary browser component, Microsoft bundles [AOL] in the "Online Services Folder" on the Windows desktop. . . . Microsoft has made it clear that they will not continue to include us in Windows if we don't agree to continue our 'virtual exclusivity' provisions for use of IE within [AOL]. . . . [O]ur present intent is to continue with IE, partly to get the continued marketing benefits of Windows bundling, and partly to maximize the likelihood of continued 'detente' with Microsoft"); *see also id.* at 80 (quoting Microsoft Chairman Bill Gates as stating, "I do recognize that, by choosing to [use the "Windows Box" for the browser battle], we have leveled the playing field and reduced our opportunities for competitive advantage with MSN").

[49] WebSideStory Press Release, *Netscape's Browser Share Would Rise to 20 Percent Worldwide if AOL Converted its Customers to Netscape* (May 1, 2001), *available at* http://www.Websidestory.com/cgi-bin/wss.cgi?corporate&news&press_1_130.

market share (19.5%) little different from IBM's market share in operating systems at the time of the Justice Department's 1994 consent decree (17%); and Microsoft's browser market share would be higher than its operating system market share in 1994 (80% versus 79% excluding Apple).

The 6.5% market share attributable to AOL today is strikingly lower than the 15% which it accounted for only two and a half years ago, in November 1998, when browsers were less ubiquitous.[50] It also provides a useful point of comparison for considering the likely trajectory of market share as other Web-based applications, such as instant messaging, grow from early adoption to universal usage. AOL, for example, which pioneered important developments in instant messaging, currently has a 51% IM market share and 23 million users, according to the Gartner Group (Microsoft's market share is 36% of consumers and 40% of business users).[51] This 23 million installed base, however, is dwarfed by the 180 million users who are expected to use IM within the next three years[52] -- not to mention the 160 million PCs that will ship with Windows (and hence MSN Messenger) next year alone.[53]

---

[50] *See United States v. Microsoft*, 84 F. Supp. 2d at 84 (quoting AOL estimate in November 1998 that its switch from IE to Navigator would effect a 15% change in market share, from 50/50 to 65/35).

[51] Gartner Press Release, *Gartner Examines Microsoft Versus America Online Impending War in Instant Messaging and Web Services Space* (May 1, 2001) (AOL has 23 million users), *available at* http://www4.gartner.com/5_about/press_room/pr20010501a.html; Gartner Press Release, *Gartner's Instant Message Survey Shows America Online Leading Microsoft* (May 1, 2001) (AOL has 51% consumer market share versus 36% for Microsoft; and 52% business market share compared to 40% for Microsoft), *available at* http://www4.gartner.com/5_about/press_room/pr20010501b.html.

[52] *Gartner's Instant Message Survey, supra.*

[53] Jay Greene, *Microsoft: How it Became Stronger Than Ever*, Business Week (June 4, 2001), at 79.

Only Microsoft's Windows, Internet Explorer, and Office monopolies have such universal reach. AOL, for example, has no real presence in the business environment, where all three Microsoft monopolies are omnipresent. As much of the growth in IM will come from business users -- IDC predicts that IM corporate use will grow 140% a year, from 5.5 million in 2000 to more than 100 million in 2004[54] -- Microsoft can be expected to gain the overwhelming percentage of those users. As the *Wall Street Journal* recently observed:

> America Online, despite its early lead in instant messaging, hasn't made significant inroads in corporations. Microsoft, whose software is on nearly every corporate desktop, could build a vast instant-messaging service by wooing business customers. . . . The technology, once limited to a young, chat-happy audience, promises to become one of the most significant new platforms for communications. While programs like spreadsheets and word-processing applications help boost the fortunes of technology companies in the 1990's, "now, instant messaging is the killer app," says Rick Sherlund, a Goldman Sachs analyst.[55]

Any effective alternative to Internet Explorer (which, in Windows XP, is now also the Windows user interface) would have to be able to compete head-on in this business market. In considering potential remedies to Microsoft's browser monopoly, accordingly, it is important to consider how successfully a competitive alternative might be able to penetrate this market -- and it is in this regard that the proposed structural separation of Windows and Office has appeal.

---

[54] IDC Press Release, *Corporate Instant Messaging Will Grow at a Strong Rate but Faces Obstacles* (Oct. 24, 2000), *available at* http://www.idc.com/software/press/PR/SW102400pr.stm.

[55] Julia Angwin and Rebecca Buckman, *How Microsoft's Messaging Could Leapfrog AOL's*, Wall Street Journal, B1 (June 19, 2001).

Microsoft itself, by its design choices, recognizes that Office is a powerful platform for the distribution of these technologies. Office XP, for example, is the only other product to which Microsoft has attached its SmartTags scanning program. In Microsoft's hands, combining SmartTags with both Internet Explorer *and* Office enables Microsoft potentially to reach nearly all content viewed by computer users -- nearly 90% of all Web pages that users see, and more than 90% of the content that they create. As one reviewer of Office XP noted:

> Microsoft is unabashedly using [SmartTags] to tie its Office customers into its growing stable of Web services. Stock reports, for example, come from MSN MoneyCentral, and tags for famous names point to further information on Microsoft's Encarta site. . . How one feels about all this depends not just on your reaction to the individual sites and services involved, but also on your overall assessment of Microsoft and its .Net strategy -- its emerging plan to extend its domination of the software market to the Internet by providing free and, eventually, subscription services. At a minimum, it seems undeniable that with Office XP, Microsoft is again using its power in an established market to give itself a huge head start in a new arena.[56]

In the hands of a competitor, however, Office has precisely the opposite effect: SmartTags potentially directs users to *non-Windows* services and sites. Similarly, Office XP incorporates instant messaging capability into its suite, with instant messaging necessary in order for the user to take advantage of certain Office features. Office thus provides a ready distribution channel for competing IM services, as well as an alternative source of global identity. And, finally, Office would be a plausible rival to Internet Explorer as a platform for Web service APIs: with a market

---

[56] Henry Norr, *Software Boasts Valuable Changes*, San Francisco Chronicle (May 31, 2001) at C6.

penetration of many tens of millions of desktops, it would offer distributed application developers a potential choice of program interfaces available on the desktops of their users.

* * * *

In the event Microsoft is found to have engaged in illegal conduct under the Sherman Act in the pending litigation, the potential for separating Office and Internet Explorer/Windows should be considered. They would appear to be the products most capable, inside Microsoft or out, of competing to serve as the principal user interface for accessing the coming generation of distributed applications -- a new world of Web-based services that will transform how users communicate, engage in commerce, and collaborate with one another. On remand, issues might need to be carefully considered regarding whether and how particular services and programs should be divided to further facilitate the creation of such competition. What would appear clear, however, is that the emerging world of distributed applications should benefit from the innovation that attends the competitive process. Control of these markets by a single company not only would have a likely deleterious effect on this innovation, but also would remove the competitive pressure that helps to ensure that companies do not misuse their market position in other ways. In the absence of such competition, the only alternative to the discipline of the market is government oversight -- an alternative that surely no one prefers. For that reason, and given the serious risk that the failure to impose an effective remedy will lead to that outcome, serious consideration should be given to a structural remedy that might hold out the prospect of ensuring competition in these markets in the years to come.