Stephen Streiker,
Esquier, Attorney, Los Angeles

ANTITRUST ENFORCEMENT IN A NEW AGE ECONOMY

This paper addresses issues of large international dominance by Microsoft in software and browser platforms and American Antitrust Law and its ability to curb and deal with those abuses.

I. Introduction The Way We Were. Looking back on the Microsoft Consent Decree against the current marketplace background:

A. The ten year anniversary a time to look back

As we approach the ten year anniversary of the Findings of Fact [1] in landmark antitrust case against Microsoft [2], it is interesting to step back and look as the case, its process, its results, and more importantly its impact to the industry. Things have changed in the world of software distribution dramatically in the last ten years. When one evaluates the case, its remedies and the current marketplace it is clear that the antitrust enforcement channels are simply not effective in today's "New Economy" industries that move at the energetic pace of the technology sector of the 21st Century.

Damage to the competitive playing field was rapid before the Microsoft Consent Decree. The restrictions placed on Microsoft were largely ineffective in dealing with the more leisurely rate of market uptake. Today's software market adoption rate is ruled by a lightning fast pace of change and consumer uptake. Antitrust enforcement is not up to the challenges faced by a market that change overnight with a click of a mouse. The software marketplace is framed by significant antitrust actions. In the last twenty years Microsoft has been the target of two significant antitrust enforcement actions in the United States stemming from their abuses of their long dominance in the markets for PC operating systems. Additionally they have been the target of competition regulation authorities in several foreign jurisdictions with several significant investigations and enforcement actions brought against them. Microsoft has entered into two significant consent decrees settling cases with the U.S. Justice Department and limiting their actions, one in 1995 and one, which they still operate under court supervision dating to 2001. These consent decrees largely are backward looking limiting conduct engaged in the past. It is ten years from the original Findings of Fact in the most significant antitrust case they face but today we find ourselves and Microsoft facing a much different world. A world where continued anti-competitive behavior can more quickly propagate distort consumer behavior in relevant markets for software uptake. Today we have factors that accelerate the rate of software adoption and consumer uptake: Cloud Computing, Software as a Service (SaaS) [3], an internet connecting billions more consumers literally at just the click of a mouse. Microsoft and other key dominant players like Google and Yahoo have the tools available to lock-in markets and to amplify outcomes at a rate

unimagined even just five years ago. Are the restrictions and enforcement régime crafted ten years or so reacting to their anti-competitive contracting and marketing practices of fifteen to twenty years ago up to the challenges of the New Economy? Is the antitrust regime that presumably limits the actions of large market share players like Microsoft and Google up to the challenge of today's marketplace that is as different today from 1995 as 1995 was perhaps 1960 when it comes to consumer software distribution?

The ten year anniversary of the antitrust litigation that stemmed from "The Browser Wars" of the 1990s offers a good vantage point for questions to be asked about the future of antitrust as it relates to the ability of the antitrust machinery to effectively react and play a positive role in preserving the competition that insures the maximum value for consumers. Is there a role to play for antitrust to protect software consumers in the future? Is antitrust simply too lumbering, slow moving to deal with the pace of anti-competitive market behaviors engaged in by dominant players and the lightening fast consumer uptake in today's Internet friendly, cloud-computed, instant download world? Do Congress, the courts, the Department of Justice Antitrust division and competition authorities in the EU and around the world to find better ways of insuring that innovation in software markets is not harmed by rapid deployment of locked in IT software monocultures. Are today's laws and enforcement machinery up to the challenges of a marketplace that has an unprecedented rate of consumer uptake which is increasingly dominated by a few powerful players?

We are going to argue that there IS a role for antitrust enforcement but the track record of enforcement shows that there is an urgent need for reforms to the scope and pace of antitrust enforcement dealing with the behavior of dominant players lest long-term damage is done to some key software marketplaces. There are indications that the U.S. antitrust enforcement machinery and laws just are not up to the challenge presented by the potential rate which a monopolist's conduct can propagate through the markets for some especially key PC applications software, most notably, security software.

B. Question presented

Can the current antitrust laws and enforcement machinery effectively deal with the rapid rate of consumer uptake in software markets dominated by the largest market players.

C. Short Answer

No. In spite of the highly visible enforcement action aimed at Microsoft's monopolist conduct Microsoft has emerged stronger and more entrenched in its market presence. Additionally Google has emerged as a dominant force in the search industry. The rise is cloud computing and new models of distributed application software provision raise interesting questions about how government can foster a free market system in market sectors that could increasingly be driven by two major dominant market participants.Looking back on Microsoft v Netscape.

In the 1990s Microsoft used its market dominant power to subvert the entrance of two possibly formidable competitors: Netscape, Inc.'s Netscape Internet browser and Sun Microsystems, Inc. Java applications execution environment. Microsoft's conduct in dealing with this "Middleware Threat" [4] lead to antitrust action in the United States and other jurisdictions around the world.

D. The rise and fall of Netscape as a 'middleware' competitor

On October 16, 1996 Charlie Rose interviewed Netscape co-founder, Senior Vice President at Chief Technical Officer Mark Andreessen about the bright prospect for both Netscape's browser [5] and back office server software businesses [6]. Microsoft responded to the early success of Netscape's flagship software product, an inexpensive (about $49 per user at retail, less in corporate and academic environments) well designed and implemented Internet Browser by licensing an earlier version developed by the Netscape browser team when they were at the University of Illinois. Building on this earlier "MOSAIC" browser Microsoft rolled out its Internet Explorer 1.0 and made it available free to all users of its market dominant Windows operating system. Andreessen painted a bright picture about Netscape's prospect to gain significant share of what he estimated would be a $10 Billion (USD) business in just four years.

Charlie Rose asked Andreessen, who at that time had a $300 million annual sales business with supposedly unlimited prospects, "how scared are you of the competition: Microsoft?" Andreessen's response, tossing off any real concern that Netscape's 80% share in browser software would be effectively challenged was, "we'll see what happens." Well, today we know 'what happened' to Netscape: By the end of 1998 what was left of a company that of the once had most sought after stock on Wall Street was sold to AOL for $4.2 billion. Shareholders received no cash but only stock in AOL, a currency that would soon be worth much less as AOL's fortunes diminished rapidly [7]. Most of that value being in the 'Netscape' brand and advertising traffic flowing to various Netscape advertising ventures and by 2000 there was no more Netscape as a viable independent company. Microsoft by 2000 had pretty much owed the browser marketplace not only for Windows machines but also in the Mac computing space.

Despite once having a nearly 90% share among users of internet browser software [8] and a record first day 'pop' of $75 per share on its first day of trading following its initial public offering Netscape was essentially a corporate corpse by 1999 when it was sold to AOL. AOL announced the end of support for the last browser carrying the Netscape name recently. Microsoft had won the 'browser wars' of the 1990s and its Internet Explorer, which it had never charged users to use, was by far the most use browser in the world.

Despite competition from Apple's Safari, Mozilla, Chrome developed by Google and a handful of other open source browsers was dead. Microsoft had seen the writing on the wall in the 1990s and acted decisively to fight against many types of computer 'middleware' that could make user applications more portable across different operating systems (one threat that browsers that had the same user experience look and feel across different computing platforms like Apple Macintosh, Linux, Unix and Windows). A series of OEM licensing restrictions and marketing practices that were part of Microsoft's licensing and contracting environment finally brought the attention of Antitrust, national competition authorities and states' Attorneys General.

E. The damage from anti-competitive activities occurred very quickly even before the rise of Net 2.0. Today all it takes is a click of the mouse to obtain a software application

Even in those early days of the Internet boom where most net users depended on dial-up modems and software largely distributed in the mail or through retail stores of floppy discs Microsoft had used its market dominating fire-power to strangle a potential long-term competitor in the cradle. Netscape, a fast growing software competitor, the darling in the media with a well regarded team of top software engineers, marketing professionals and solid venture capital backing was soon just a footnote in the history of Microsoft's efforts to target upstarts in their immediate vicinity. In 2007 AOL stopped offering even minimal support for browsers software bearing the Netscape name. Keep in mind that in 1997, during the middle of the "Browser Wars" there were perhaps 70 million Internet users [9], with most tethered to rater slow dial-up connections. Most users in those days loaded software applications from floppy disks. It would often take hours to download a software application such as Netscape if you chose to load it onto your computer that way. Today, with the pace of software distribution is accelerated to an unprecedented rate. There are nearly two-billion internet users[10] and increasingly, most of these users have access to the Internet using high-speed digital connections offering the ability to nearly instantly download software applications with just a click of the mouse. Microsoft's conduct, which was later ruled as precluded anticompetitive behavior worked quickly against competitors in the late 1990s, the potential for mischief due to anti-competitive behavior, is just amplified many times over due to the speed and technological scale of today's internetworked computer infrastructure.

It is becoming widely accepted that interactive networks amplify the effect of abusive multi-tying, bundling, predatory pricing and dominant OS leveraging [11]. For over a decade, Microsoft Corporation has faced antitrust challenges to its tying, contracting, pricing and abusive contracting practices that reinforce and extend its market dominance, issued by governments as well as competitors and consumers worldwide [12]. Microsoft has triggered antitrust and competition authorities action in the U.S [13], Japan, Taiwan, South Korea [14], and the EU [15].

F. Microsoft sanctioned by antitrust authorities

Microsoft did not go unpunished. Yes, the antitrust authorities observed the events and behaviors by Microsoft that were eventually ruled to be illegal conduct contrary to Section 2 of the Sherman Antitrust Act [16]; and, yes, Microsoft was punished by saddled with a set of remedial restricts on its future conduct. Microsoft sinned, was caught and punished but did not bring Netscape back from the dead or put the marketplace for computer middleware that could threaten its entrenched operating system monopoly back to the point where Microsoft's OS monopoly faced series competition from operating system agnostic middleware vendors. The history of the Microsoft case, it's conduct in the marketplace, then and now, and the failure, largely, of the remedial efforts to keep history from potential repeating itself is a

concern to the long term health of the entire worldwide network of computing infrastructure.

The tale above, recounted in dozens of magazine articles, law review journals, provides a cautionary tale to consumers and vendors concerned for a vibrant effective and competitive future for software applications that secure both individual PCs and the greater Internet's complex infrastructure. Exclusion of vibrant competitors from this key area could have significant negative ramifications to a U.S. and world economy increasingly dependent on secure and healthy computing and IT network infrastructure.

G. The backward looking remedies were largely ineffective; more proactive and forward looking remedies necessary in the future

Provisions were put in place to circumscribe Microsoft's *future* conduct but the effects of their *past* conduct was largely locked in by then. More than one observer has found not just failures of enforcement of the Consent Decree [17] but a general failure of the remedial actions that Microsoft did observe to do much of anything to restore any competitive threat to Microsoft. The process has been costly with an army of lawyers, Microsoft staffers and others engaged for now nearly twenty years in litigation and compliance efforts [18].

Well summed up by Transamerica Professor of Business Strategy at the University of California at Berkeley Carl Shapiro in his paper *Microsoft: A Remedial Failure*:

Looking back after six years, the Final Judgment has achieved precisely what it was designed to do: prevent Microsoft from continuing to engage in the conduct that *had* been found to be illegal. The Final Judgment has *done nothing significant to affirmatively restore competition* [emphasis added] [29].

Shapiro and others agree that the settlement looked *backwards* to what Microsoft *had* done and not in any way forwards towards conduct that would allow vibrant competition that could seriously threaten Microsoft's monopoly dominance.

No real end is in sight and some have wondered how a remedial plan could be such a failure [20]. It has been observed that the Microsoft antitrust enforcement action ended not with a bang, but, alas, with a whimper [21].

H. Central Question: Can the current US antitrust laws effectively regulate potential monopolists in a market that moves at speed of light?

This is the issue: Is the U.S. antitrust machinery – which often moves at was has been described at a 'glacial pace' [22] - up to the challenges of reigning in market dominant software application suppliers who have access to potentially billions of computers with only a couple of mouse clicks?

The short answer to the question posed is NO. The New Economy presents a different environment where delayed action is essentially no action. There has got to be a better balance of proactive monitoring, aggressive response to anti-competitive actions by market dominant players. The current climate of slow antitrust response is fraught with risk and is not acting in a way to bring forth any meaningful change in the conduct of high market-share participants.

Eminent antitrust scholar Judge Richard Posner has written on this topic suggesting some steps to bring antitrust enforcement into more congruence with the pace of change found in the New Economy but

admits, “the measures that I have suggested, even if all were adopted would probably not fully correct the serious mismatch between the conditions of the new economy and the institution structure of antitrust enforcement” [23]. While Judge Posner does throw up his hands a bit over this mismatch in the pace that the New Economy and IT technology unfold and the exceedingly slow pace of enforcement and litigation in U.S. antitrust he is not in favor of abandoning antitrust oversight of the activities of fast moving technology companies. “I think a policy of zero enforcement against alleged exclusionary practices in the new economy would be a mistake, however, because there is a pretty solid theoretical basis for concern both that some new-economy first would find it in their rational self-interest to employ such practices and the natural market forces would not undo those practices in time to avoid significant social costs” [24].

While some scholars have suggested that antitrust enforcement for fast moving technologies is inefficient and an unwarranted drag on innovation in key important markets there are proposals for reform including modernizing the antitrust trial format itself to lead to swifter and more accessible enforcement of the U.S. Antitrust laws [25]. Posner and others recognize that the traditional anglo-American traditional court trial does not serve such specialized and technical litigation as is found in most antitrust actions [26]. Some U.S. antitrust actions have dragged on for nearly a generation before resolution or until the companies being investigated fell victim to changing marketplaces and went out of business [27]. Some people think that antitrust enforcement in high tech is just a drag of innovation and on the U.S. Economy as that it should be scaled back with regard to IT and high tech businesses. Jonathan Baker of The Brookings Institution has observed that “critics [of current antitrust enforcement efforts] central claim that the pace of change in high tech is so rapid that antitrust, and the legal machinery within which must operate, is too slow and potentially counterproductive” [28].

In 2002 Congress established an Antitrust Modernization Commission to address whether the antitrust laws need to be changed in light of globalization and rapid technological change [29]. Joel Klein, the former Assistant Attorney General at the DOJ Antitrust Division and lead lawyer in the litigation against Microsoft has acknowledged that“ [o] ur economy is in the midst of dramatic changes, with increased globalization and rapid technological innovation…” and that antitrust law must see reform to keep up with these changes [30]. Klein has admitted in a speech at the Woodrow Wilson Center’s progam on “Sovereignty In the Digital Age” that the pace of antitrust enforcement has got to keep up with the speed as which the global economy currently moves [31]. Frankly not much came from either Mr. Klein’s recommendations or the action of the Antitrust Modernization Commission. The pace of antitrust enforcement in the United States is exactly where it has been since it was at the rise of the industrial age and the creation of the Sherman Act.

Antitrust is not completely dead in this high-tech age. Competition is, almost all agree, vital to ensuring the continued rapid pace of

innovation in IT but is the current pace of the antitrust enforcement process up to the demands of markets that face lightening fast change? Perhaps not, and perhaps it is time for a legislative review of what could be done to reform the current system to give antitrust enforcers and the courts the rapidly deployable tools to deal with markets as we find them today?

It is time for Congress and the Courts to look at the governmental machinery of antitrust and upgrade it for the demands of today's "New-Economy."Why overall market dominance by Microsoft or any other provider should not be allowed in the security software market space.

I. Antitrust regulators have to adopt a more proactive approach to prevent the dangers of software monoculture

Antitrust regulators must be especially vigilant to a threat to once competitive markets: Monoculture. In today's world where market for consumer software is increasingly one of rapid software adoption innovation can be stifled by rapid extermination of competitors by the market dominant players.

J. The Monoculture Problem

It is tempting for a farmer to select the crop seed that produces the highest crop yield per acre when planning his or her spring planting [32]. Tending one crop would like require a lower investment in farm implements, a single plan for cultivation, weeding and harvesting. In theory a farmer would just look at which crop is likely to give the largest pay off at harvest and plant every acre on his farm with that crop. If you have visited a farm in the American Midwest you'll know that that isn't what is done. Usually no more than a quarter of the acreage is committed to a single hybrid seed of any crop Usually one farm will have more than one crop planted. Some land is planted in corn, some in sorghum or soybeans or even hay. Even if large parts are planted in one crop like corn the farmer will likely choose two or more biologically diverse corn seed hybrids with different characteristics. Why?

The reason why is because if one crop were chosen you would run the risk that a single plant pathogen, disease, fungus, weather event could wipe out the entire crop which could be vulnerable to that attack. **Monoculture** is the agricultural practice of producing or growing one single crop over a wide area [33]. Computing infrastructure reacts much like a plant community. A single software application widely adopted could subject many users spread over a large area to a successful disabling attach from a "computer pathogen" like a virus or other network borne attack.

1. The network is threatened by monoculture

It cannot be ignored that the sum of the world's computers is a rapidly increasing force multiplier [34]. This "force multiplier" can be used for both good *and* ill.

In biological systems, agriculture, and computer system infrastructure 'mono-culture' is not a good idea. Failure to diversify and deploy different security solutions to protect different parts of the network makes it easier for a single threat, attack or malevolent application to initiate a 'cascading network failure.' Having multiple security solutions engineered by independent developers, each with a different approach and unique security safeguards makes it

difficult for the author of a single threat to penetrate the protections. The information technology industry, as many observe, consists of a rapidly evolving and highly interconnected network of organizations, technologies, products, and consumers and it is likened to a similarly interdependent and complex biological 'ecosystem' [35]. Just as biological ecosystems can be threatened to a monoculture of biological defenses, the IT ecosystems is threatened if the organic defense mechanisms are not varied and widely distributed. More diverse security solutions widely dispersed across different systems with different methodologies and different strengths and weaknesses are better than one monolithic security solution that once figured out by an attacker would lead to every network or every machine on the worldwide IT infrastructure being compromised simultaneously. *This, clearly, is not desirable, and needs to be actively prevented.*

K. Why it is desirable that users are protected by diverse set of competing PC and network security solution providers

Antivirus (or anti-virus) software is used to prevent, detect, and remove malware, including computer viruses, worms, and Trojan horses. Such programs may also prevent and remove adware, spyware, and other forms of malware. The current marketplace supports several vendors, each utilizing different approaches and computer code to provide what most if not all agree the much needed protection from the large numbers of threats. Individual user PCs connected to the Internet are subject to possibly thousands of new threats every day. Even *the language* chosen to describe computer security threats parallels the discussion of biological disease threats – "virus," "worm" etc. Anti-virus and other PC and network security software protects from the "pathogens" developed and propagated in the network biosphere.

Deploying a particular anti-virus or security solution application on a particular PC is much like selecting a single disease resistant hybrid crop seed. It may do an excellent job as defending that PC against a wide range of security threats (the pests, diseases and pathogens of the computer and network eco-system.) Users are usually protected well by their choice but all users shouldn't choose the *same* internet security solution anymore than farmers should plant all of their crops using the same seed hybrid. The risks are just too great. Eventually even a good security solution will be breached. If different users choose diverse security solutions we can usually be assured that no *one* threat can pose a risk to the *entire* network. It is much harder to craft a virus, malware, Trojan or worm that could simultaneously defeat *all* available defenses across several vendor's security software. This is why it is important that no one single security vendors achieve a large or monopoly position in this critical space.

In short, a network environment where all computers are protected by a single security application are vulnerable to the same viruses and other threats at the very *same* time. One attack wipes out your entire computing infrastructure simultaneously. This is a risk that is unacceptable to most single enterprises and is an especially daunting prospect when considered across the entire network.

In a paper delivered to the Computer & Communications Industry Associations General Meeting 2003 the authors, leading experts in network security, observed".

- Our society's infrastructure can no longer function without computers and networks.
- The sum of the world's network computers is a rapidly increasing force multiplier.
- A monoculture of network computers is a convenient and susceptible reservoir of platforms which to launch attacks; these attacks can and do cascade.
- The susceptibility cannot be mitigated without addressing the issue of that monoculture [36].

The authors of this paper agree that "risk diversification is a primary defense against aggregated risk when that risk cannot otherwise be addressed." They and others understand that a security software monoculture creates rather than eliminates risk.

L. There is a bias towards software monoculture due to Network effects in the adoption of application software

1. What is a Network effect

If the world had only a single telephone, that telephone would not be very valuable, after all you wouldn't have another telephone to connect to and talk to another user [37]. Network effect can be explained as: the greater the network of users of a certain product, the higher the utility of the used product (the more the better). As a network of people who use the same product expands, the communication among consumers using the same product such as a PC operating system or spreadsheet-application becomes more accessible [38]. This is the 'direct network effect' of economics. Consumers tend to adopt solutions that are chose by many other consumers, even if they are not the ideal solution to a problem. Additional value is gained by using a software application chosen by a lot of other people.

2. Crushing wins are nurtured by 'network effects' and the winner can become 'locked in'

Microsoft and other companies who already exercise large amounts of market power often key their marketing to take advantage of network effects. Once a standard is set and a dominant application fills a market space it can and is very difficult to unseat an incumbent in a particular computer application space. We would argue that Antitrust authorities have to adopt strategies to monitor crushing wins in certain critical computer application market spaces; computer security software being one of those.

3. Lock in – One application can end up with nearly 100% of the marketplace

It is widely accepted that computer software network effects lead to a 'lock in' of often only one dominant software application. There are very strong network effects operating in the market for widely used computer software. Often cited, for example, Microsoft Office. For many people choosing an office suite, prime considerations include how valuable having learned that office suite will prove to potential employers, and how well the software interoperates with other users. That is, since learning to use an office suite takes many hours, they want to invest that time learning the office suite that will make them most attractive to potential employers (or

consulting clients, etc), and they also want to be able to share documents. Additionally, an example of an indirect network effect in this case is the notable similarity in user-interfaces and operability menus of most new software - since that similarity directly translates into less time spent learning new environments, therefore potentially greater acceptance and adoption of those products [49].

Similarly, finding already-trained employees is a big concern for employers when deciding which office suite to purchase or standardize on. The lack of cross-platform user-interface standards results in a situation in which one firm is in control of almost 100% of the market.

Microsoft Windows as was recognized by the DOJ and the court in *Microsof* [40] is a further example of network effect. The most-vaunted advantage of Windows, and that most publicized by Microsoft, is that Windows is compatible with the widest range of hardware and software. Although this claim was justified at some point of time, it was in reality the result of network effect: hardware and software manufacturers ensure that their products are compatible with Windows in order to have access to the large market of Windows users. Thus, Windows is popular because it is well supported, but is well supported because it is popular [41].

4. And this leads to the tipping effect

As users increasingly get 'locked in' to a particular application a point comes where the marketplace for that particular marketplace becomes 'tipped'. A cascade effect will take over and the demand of users will lead to a particular application becoming the widely preferred product [42]. Operating system vendors (OS) can even use this to lock in users of their particular OS. Jung Wook Cho in *Innovation and Competition in The Digital Network Economy* points out that this effect in applications can further accelerate a OS lock in saying, "… this tipping effect may even more [be] reinforced by indirect network effects. For example, if a number of [software application's that run well only on one OS] users increase, the number of consumers connected to Window PC OS network is likely to increase as well" [43]. Tipping can and does occur very rapidly [44]. locking in a market leader even in the face of later superior products.

M. Predatory Pricing leads to monoculture

One tool repeatedly used by Microsoft and other market dominant monopolists is predatory pricing [45]. It is settled law that predatory pricing is illegal under American Antitrust law [46]. With low marginal unit costs of selling a new unit of software (after all all of the code was written and already paid for in the past, producing and delivering a new customer an existing software application is close to zero) is essentially zero. In the new-economy there is even a *greater risk* of predatory pricing being used as an anticompetitive exclusionary tool than in old-economy industries [47]. Predatory pricing can be an illegal tool under the Sherman Act that could create a software monoculture and to defend that monoculture turf once captured [48].

1. Predatory Pricing at an anticompetitive tool

Predatory pricing is the practice of selling a product or service at a very low price, intending to drive competitors who have less deep pockets out of the market, or create barriers to entry for potential new competitors. If competitors or potential

competitors cannot sustain equal or lower prices without losing money, they go out of business or choose not to enter the business. The predatory merchant then has fewer competitors or often even de facto monopoly in a particular market space [49]. The danger posed by predatory pricing is that once the well-healed competitor drives out other less well-funded competitors then they could harm consumers by raising prices above what the market would otherwise bear. While presumably any competitor could attract market share to a very low price a competitor with very high market power, financial resources or market motivations beyond just the relevant market can call on those external resources and benefits to ride out the period of financial loss while other smaller players cannot. Once they are gone, the theory goes, the predatory pricer (the "monopolist") can reverse course and make up for any earlier losses by overcharging consumers now that they have the market to themselves. Economists like to sum up predation as follows: an act (by a monopolist) if it "involves a deliberate sacrifice of profits in order to gain or protect monopoly rents as opposed to gaining of rents though superior skill, foresight and industry" [50, 51].

The use of predatory pricing is a disfavored strategy under U.S. and other jurisdictions antitrust and anti-competition laws [52]. In antitrust cases the courts "interpret §2 of the Sherman Act to condemn predatory pricing when it poses "a dangerous probability of actual monopolization" [53, 54] In the original *Microsoft* decision the district court judge found that Microsoft lost money while trying to gain market share from Netscape in its attempt to monopolize the browser market by leveraging its monopoly of the OS market [55]. Microsoft has been criticized for using 'free' distribution of software as an unfair predatory practice [56]. One can argue that free distribution is good for consumers but it is recognized that pricing practices by a dominant company, even free distribution, are often another manifestation of abuse of dominance [57]. As Professor Cho points out in his well regarded work, *Innovation and Competition in the Digital Network Economy: A Legal and Economic Assessment on Multi-tying Practice and Network Effects,* Microsoft has *already* been accused of predatory pricing in the security software market not only in the United States (June 2006) [58], but also in Europe (September 2006) [97]. Microsoft's predatory pricing (free distribution) of Internet Explorer played an important part in leveraging it's OS monopoly into a dominant share of the relevant market for browsers. Can the competition authorities and competitors in the very important market space of security software stay asleep at the switch. We would argue that they cannot. Predatory pricing by a dominant market player like Microsoft or Google or perhaps another SaaS provider can play a powerful part in allowing a dangerous software monoculture to come into being in security software.

2. The use of free distribution by market dominant players should be scrutinized carefully by antitrust and competition authorities to prevent its use to move software markets towards monoculture

Free distribution is not *per se* improper and is often a viable an important tool for marketing for many software publishers but

it's use in the hands of monopoly or high market share organizations as a illegal predatory tool needs to be looked at carefully to prevent illegal abuse and extinction of critical diversity and innovation in key markets like security software.

N. The monoculture problem as it relates to security software

It is especially important that Internet security applications be protected from the emergence of a software monoculture. Reduction in innovation and consumer choices poses more than just a business threat to the competitors in the market space for Internet security software; it poses a real danger to the integrity of the world's networking infrastructure.

1. Why it is desirable that users are protected by diverse set of competing PC and network security solution providers

Antivirus (or anti-virus) software is used to prevent, detect, and remove malware, including computer viruses, worms, and Trojan horses. Such programs may also prevent and remove adware, spyware, and other forms of malware. The current marketplace supports several vendors; each utilizing different approaches and computer code to provide what most if not all agree the much needed protection from the large numbers of threats. Individual user PCs connected to the Internet are subject to possibly thousands of new threats every day. Even *the language* chosen to describe computer security threats parallels the discussion of biological disease threats – "virus," "worm" etc. Anti-virus and other PC and network security software protects from the "pathogens" developed and propagated in the network biosphere.

Deploying a particular anti-virus or security solution application on a particular PC is much like selecting a single disease resistant hybrid crop seed. It may do an excellent job as defending that PC against a wide range of security threats (the pests, diseases and pathogens of the computer and network eco-system.) Users are usually protected well by their choice but all users shouldn't choose the *same* internet security solution anymore than farmers should plant all of their crops using the same seed hybrid. The risks are just too great. Eventually even a good security solution will be breached. If different users choose diverse security solutions we can usually be assured that no *one* threat can pose a risk to the *entire* network. It is much harder to craft a virus, malware, Trojan or worm that could simultaneously defeat *all* available defenses across several vendors' security software. This is why it is important that no one single security vendors achieve a large or monopoly position in this critical space.

In short, a network environment where all computers are protected by a single security application are vulnerable to the same viruses and other threats at the very *same* time. One attack wipes out all of your computing infrastructure simultaneously. This is a risk that is unacceptable to most single enterprises and is an especially daunting prospect when considered across the entire network. In a paper delivered to the Computer &Communications Industry Associations General Meeting 2003 the authors, leading experts in network security, observed".

- Our society's infrastructure can no longer function without computers and networks.

- The sum of the world's network computers is a rapidly increasing force multiplier.
- A monoculture of network computers is a convenient and susceptible reservoir of platforms which to launch attacks; these attacks can and do cascade.
- The susceptibility cannot be mitigated without addressing the issue of that monoculture [60].

The authors of this paper agree that "risk diversification is a primary defense against aggregated risk when that risk cannot otherwise be addressed." They and others understand that a security software monoculture creates rather than eliminates risk.

O. Microsoft has the ability and inclination to leverage its marketplace power to effectively exclude rivals from the internet security space

George Santayana (1863 1952) [61], Spanish philosopher, essayist, poet, and novelist is often paraphrased in his observation that "Those who cannot remember the past are condemned to repeat it" [62]. Even after repeated anti-trust sanctions, consent decrees and competition authorities actions in the United States and around the world Microsoft continues to show a clear pattern of corporate "personality" that revolves around leveraging their consumer dominance in the computer operating system marketplace to win crushing victories in market share in other categories of computer applications.

Not preparing for further conduct by Microsoft in any software category which they have decided to enter and dominate would be a mistake. They've utilized their market exclusionary power before and despite strong sanctions they likely will again. Other commentators have also observed that Microsoft, without dramatic change to its corporate organization or conscious and well though-out steps to counter its monopoly dominance will pose a growing security threat to consumers and the world-wide Internet at large [63].

One need only to look at the long road littered by the corpses of once successful providers of Windows applications who found themselves and their particular markets subject to takeover by Microsoft. Word Perfect (word processing), Lotus 1-2-3 (spreadsheets), Netscape (browsers) are all names that anchored competitive application product categories whose businesses were subject to the market exclusionary and predatory conduct of Microsoft. Microsoft when it does target an application space is usually not shy about adopting strategies that would allow it to fill that application space, and if possible, push out all other competition. Against that backdrop consider that Microsoft has decided to enter the security applications arena.

Microsoft, after largely leaving the anti-virus and PC security application market to others including among others, McAfee, Symantec, AVG, has announced that it will deploy Microsoft Security Essentials (codenamed Morro) a free antivirus software providing protection against viruses, spyware, rootkits, and trojans for Windows XP, Vista.

Microsoft has a long history of engaging in exclusionary conduct which distorts the effectiveness of the marketplace. This is not just a threat to their competitors who should have to compete hard to win and retain market share for their individual products:

This distortion of the marketplace is a market failure which can create and perpetuate a wider societal threat [64].

P. There cannot be a monoculture in security software

Security software is not just another PC application. The ramifications of a successful widespread network failure in the face of a coordinated attack on the world's computing infrastructure are frightening. The ecosystem of security precautions, network redundancy and even individual PC virus and security protection is critical to protecting the U.S. and world economy from a large scale long term simultaneous network outage or failure.

1. National security implications

a) National Security implications for the United States. If Microsoft were to wipe out competitive e ISVs this could leave the US computing infrastructure vulnerable to attack.

It has become apparent that there are national security implications for the United States and other nations to breaches in computer and network security. The U.S. and world economy, energy supply, means of transportation and military defenses are tremendously dependent on vast, interconnected computer and telecommunications networks. These networks are poorly defended and vulnerable to theft, disruption or destruction by foreign states, criminal organizations, individual hackers and, perhaps offering the greatest potential for disruption and destruction, terrorists. News reports have begun to appear of actions targeting the U.S. economy. In the last few months it has been reported that Chinese network operations have found their way into American electricity grids, and computer spies have broken into the Pentagon's Joint Strike Fighter project [65]. U.S. President Barrack Obama has acknowledged critical nature of America's digital infrastructure and the real threat to our national security of a successful broad-based attack on that infrastructure. In May of 2009 in remarks made at the White House the President stated:

[N]one of these 21st century challenges can be fully met, without America's digital infrastructure -- the backbone that underpins a prosperous economy and a strong military and an open and efficient government. Without that foundation we can't get the job done.

It's long been said that the revolutions in communications and information technology have given birth to a virtual world. But make no mistake: This world -- cyberspace -- is a world that we depend on every single day. It's our hardware and our software, our desktops and laptops and cell phones and Blackberries that have become woven into every aspect of our lives.

It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history.

So cyberspace is real. And so are the risks that come with it. It's the great irony of our Information Age -- the very technologies that empower us to create and to build also empower those who would disrupt and destroy [66].

Clearly, the stakes of a less than optimal computer and network security eco-system

are high. A computer security monoculture dominated by a single player offers those bent on the kinds of widespread catastrophic destruction that a coordinated attack on the US or worldwide computer infrastructure an much easier likelihood of success. A computer security infrastructure composed of a healthy variety of different security applications presents a much more difficult problem to an attacker or attacker.

There is a growing consensus that the stifling innovation in the security sector and actions which threaten to kill the competition in the security software space through predatory pricing in fact can threaten U.S. national security by increasing the risk of catastrophic widespread network failure propagated through millions of vulnerable PCs simultaneously [67].

b) Protection from widespread, cascading network failures.

This point cannot be lost when evaluating Microsoft's conduct within the security software marketplace. Simply put, Microsoft cannot be allowed to follow its previous course of conduct in other software applications areas where they were allowed to use their monopoly marketplace power in operating systems to leverage market dominance in adjacent areas. The 'adjacent area' of computer security is just to important to allow Microsoft to defeat the strong and competitive marketplace of multiple suppliers as it exists today in computer security applications.

Q. Monoculture in security software is not like a monoculture in word processing software. Diversity of providers of security vendors has to be proactively monitored by antitrust authorities

We cannot look at the security of the worldwide computing infrastructure without considering the impact that antitrust and competition policy enforcement have on the health and safety of the worldwide IT infrastructure. Many are coming to the understanding that "competition policy is tangled with security policy from this point on [68].

1. Preventing monoculture in critical areas is in accord with the main aim of antitrust law

Antitrust law is a set of statutes, case law and enforcement methodology designed to promote competition, and technological advances. At the core of this set of law and enforcement machinery in the U.S. is the long-stated objective of advancing consumer welfare by preserving the benefits of a competitive marketplace for customers specifically and for the U.S. economy more generally [69].

This is a danger to competitors in a particular software application market space because such tipping may (and often does) allow the application produced by a dominant company to nearly (or sometimes totally) achieve *de facto* standard for the market [70]. Microsoft knew this before the action in *Microsoft* and the consent decree. It continues as a central strategy in Microsoft's entry into marketplace and is no secret to Microsoft's competitors [71]. Google is currently the most active complainant with well placed worries that Microsoft will engineer into Vista difficulties that will hobble Google's widely distributed desktop search tools which go

beyond the web to search an individual users local PC hard drives [72].

Competition authorities have to play *their* part in preventing illegal tying, predatory pricing and illegal contracting practices from being used by large market dominant players to illicitly build a large uncompetitive market share in security software. Vibrant innovation, competition and deployment of a variety of different security software approaches are of tantamount importance to the security of the world's computing infrastructure.

An emerging view is that governments must not permit critical or infrastructural sectors of their economics to implement the monoculture path [73]. One tool towards that end is aggressive and timely action by antitrust and competition authorities – faster and more aggressive than has been the practice up to this time. Microsoft's anti-competitive behavior – Past portends future?

R. Microsoft's inclination upon entering PC security space is to dominate and exclude lesser players

While Microsoft isn't *always* successful in killing off worthy competitors in market spaces that it sets its sights on one only has to look at the battle-field strewn with casualties. Yes, Microsoft has been beaten back in *some* markets like Internet search that it was clear that it *intended* to dominate (even Microsoft can't win them all), but for every MSN, Microsoft Live or Bing there are two or three Netscapes, Word Perfects (crushed by Microsoft Word), Lotus 1-2-3s, SuperCalcs (both crushed by Microsoft Excel), dBases (crushed by Microsoft Access) or other software applications which once enjoyed market domination in their category only to have the Windows OS monopoly leveraged by Microsoft push them to virtual marketplace extinction.

S. Past anti-trust remedial action largely ineffective

Let's look at the record of recent antitrust action against Microsoft. There has been a lot of action, but largely Microsoft's monopoly power has gone unmitigated.

1. Review of cases against Microsoft

It doesn't go without note that the history of the U.S. government's antitrust challenges to Microsoft Corporation's business practices tells "a tale worthy of an epic drama" [74].

a) The Microsoft 1995 Consent Decree

Before the DOJ and several states came after Microsoft for their anti-competitive conduct towards Netscape and Sun Microsystems the company had been in the investigative crosshairs of the FTC for a decade. The FTC began investigation of Microsoft in 1990 concerned that Microsoft and IBM had agreed to limit the functionality of Windows in order to promote sales of OS/2, an operating system the IBM was developing at the time with Microsoft. The basic accusations that Microsoft was unfairly playing favorites by adding hidden APIs that were not made available to competing software vendors and with various contracting practices that raised antitrust concerns. Although the FTC dropped its investigation of several concerns [75]. the DOJ issued subpoenas and took depositions of Microsoft executives. Three companies, Novell, WordPerfect (which at the time produced, by far, the world's leading word processing program but was soon eclipsed by a large margin by Microsoft's *Microsoft Word*) and Lotus (the producer of the then market dominant spreadsheet program Lotus 1-2-3) were

successful in moving the DOJ to bring a case against Microsoft [76]. Things came to a head quickly and Microsoft, seeing the writing on the wall [77], entered into a consent decree to settle charges brought by the DOJ in response to certain alleged unlawful practices aimed squarely at Novell, WordPerfect and Lotus. Microsoft agreed to end certain illegal 'tying' provisions and marketing practices which unfairly disadvantaged the three earlier named application software providers. These restrictions were memorialized in the "1995 Consent Decree" [78] between Microsoft and the U.S. Department of Justice.

b) The current Antitrust case against Microsoft – Sometimes referred to as Microsoft III

Most observers agree: nothing much changed in Microsoft's actions with regard to competitors after the 1995 Consent Decree. Microsoft found workarounds to the Decree and mostly vanquished WordPerfect Corporation's Word Perfect word processor with Microsoft Word and Lotus's Lotus 1-2-3 with Microsoft Excel. Microsoft turned up the heat and continued to aggressively leverage its dominance in the OS market space to big wins in enterprise software for email, word processing, databases and spreadsheets.

After five years of frustration dealing with an evasive Microsoft who had some thought been flouting the 1995 consent decree (the 1995 Consent Decree) stemming from continuing accused anti-competitive behavior in contravention of the Clayton and Sherman Antitrust Acts in 1998 the United States and nineteen states' Attorneys General sued Microsoft alleging that it had monopolized the market for PC operating systems by bundling its Internet Explorer web browser to the Windows operating system and by forming exclusive contracts with computer manufacturers and others which were in illegal attempts to monopolize under by §2 of the Sherman Act [79] and illegal tying arrangements prohibited by §1 of the Sherman Act [80, 81, 82].

A remarkably brief, by the standards of antitrust trials, trial began in October 1998 with closing arguments and completion by June of 1999. Again, relatively rapidly, the presiding judge, Thomas Penfield Jackson issued findings of fact [83] that for all intents and purposes accepted the government's allegations made in their case in chief. Judge Jackson found that Microsoft in fact had a monopoly in the market for PC operating systems [84] (not a surprise to anyone, not even to Microsoft) and that that monopoly was protected by a network effect[85] which he described at "applications barrier to entry" [86, 87, 88] Judge Jackson also found that Microsoft had engaged in a broad campaign to crust the "middleware threat" [89] posed by both Netscape's Navigator and Sun Microsystems's Java platform agnostic application programming language (hereinafter "Java") to evolve into rival platform for customer PC applications.

Penfield found for the U.S. Government and States plaintiffs in nearly all allegations. He found that:

1. Microsoft had a monopoly, a large and stable market share, in the market for Intel compatible personal computers;

2. An applications barrier to entry shielded Microsoft from meaningful competition in that area;

3. Microsoft illegally used its monopoly power in PC operation systems to unfairly

exclude rivals and harm competitors in contravention of §1 and §2 of the Sherman Act;

4. Microsoft hobbled the innovation process;

5. Microsoft actions harmed consumers; and

6. Various Microsoft contracts had anti-competitive implications [90].

Judge Penfield held off on remedial actions allowing the parties to engage in a intensive series of settlement talks mediated by prominent antitrust scholar Judge Richard Posner. Those talks broke down shortly thereafter on April 1, 2000 [91].

2. Remedial action Microsoft III

After a remarkably short hearing [92] Judge Jackson issued his remedial findings essentially ordering a split of Microsoft into two separate businesses [93]: One based around the Windows OS and the other which owned the applications.

The court's findings and attempted remedial action were focused on dealing with Microsoft's conduct which, in the plaintiff's and the court's view harmed consumers by suppressing innovation [94].

a) Appeal

In June 2001, the Court of Appeals for the D.C. Circuit unanimously affirmed many of Judge Jackson's holdings, but not without reversing some of his findings [95]. The court held that the binding of Internet Explorer and Windows by various contractual and design measures [96], along with exclusive contracts with other firms were monopolistic because they threatened to prevent Netscape's browser from achieving the critical mass necessary to evolve into a rival platform that would challenge Microsoft's dominance by braking the Applications Barrier of Entry. The court also affirmed the lower court's determination that Microsoft had illegally hindered Sun Microsystems's Java middleware platform through violations of §2 of the Sherman Antitrust act [97].

Despite essentially agreeing with Judge Jackson it reversed his entire remedial order [98] and remanded the case to a different judge because of improprieties by Judge Jackson [99], for further proceedings on the remedy [100].

b) Final Consent Decree

In November 2001, the United States Department of Justice Antitrust Division and the Attorneys General of nine of the complaining states [101], later to be called the "New York Group" reached a settlement with Microsoft and proposed a consent judgment [102]. With a few changes this became the final order entered by Judge Kollar-Kotelly [103].

The remedial actions entered by Judge Kollar-Kotelly and subsequent monitoring by the judge form the restrictions which Microsoft has been bound to for the last several years.

The remedial provisions apply to both the design of the operating system in its relationship to middleware and to contractual terms affecting the development and distribution of middleware. The decree requires Microsoft to provide utilities in Windows that give computer manufacturers and users the ability enable or delete various means of access to Microsoft middleware and to designate non-Microsoft middleware to launch in place of Microsoft middleware [104]. The Federal District Court made the Final Judgment for the settlement in November 2002 [105].

c) The Consent Decree: Backward looking – not proactively oriented

Provisions were put in place to circumscribe Microsoft's *future* conduct but the effects of their *past* conduct was largely

locked in by then. More than one observer has found not just failures of enforcement of the Consent Decree[106] but a general failure of the remedial actions that Microsoft did observe to do much of anything to restore any competitive threat to Microsoft. The process has been costly with an army of lawyers, Microsoft staffers and others engaged for now nearly twenty years in litigation and compliance efforts [107].

Well summed up by Transamerica Professor of Business Strategy at the University of California at Berkeley in his paper *Microsoft: A Remedial Failure*:

Looking back after six years, the Final Judgment has achieved precisely what it was designed to do: prevent Microsoft from continuing to engage in the conduct that *had* been found to be illegal. The Final Judgment has *done nothing significant to affirmatively restore competition* [emphasis added] [108].

He, and others agree that the settlement looked *backwards* to what Microsoft *had* done and not in any way forwards towards conduct that would allow vibrant competition that could seriously threaten Microsoft's monopoly dominance. Increasingly the Microsoft settlement is being viewed as plainly ineffectual. "The settlement left competition hobbled and significant violations of antitrust law largely uncorrected"[109].

No real end is in sight and some have wondered how a remedial plan could be such a failure [110]. It has been observed that the Microsoft antitrust enforcement action ended not with a bang, but, alas, with a whimper [111].

T. A better approach is needed

Let's face it, Microsoft's domination in PC operating system market share is here to stay for the foreseeable future. They have leveraged this power to domination in areas like Internet browsing software (Internet Explorer) and the key enterprise markets for back office server software, word-processing (Word), spreadsheets (Excel), small enterprise databases (Access).

As discussed earlier certain practices by a monopoly player like a Microsoft or potentially a Google pose special risks to particular software marketplace 'ecosystems.' Some of these practice can and are monitored and subject to enforcement by antitrust and competition authorities. Among these practices are tying, illegal closed contracting and licensing practices and predatory pricing.

1. Solutions that are needed in this new age

This author proposes software markets, especially essential software markets like that for PC security software be more actively monitored and subject to enforcement action. Certain market conditions and behaviors by potential monopolist players need to be subject to automatic scrutiny in the future by antitrust and competition authorities.

a) Tripwires – automatic scrutiny of entry into critical markets to prevent growth of a monoculture controlled by dominant player (Microsoft or others).

Certain conduct should trip automatic review if engaged in by market certain suspect market participants.

(1) Free distribution

This is often an attempt by amply funded high market share players to engage in illegal predatory pricing. While this is not *per se* illegal, it should prompt immediate

and timely review by antitrust and competition authorities

(2) Rapid movement towards monoculture – especially in areas related to PC and network security

Certain key software markets should be subject to continuous and aggressive oversight to spot precluded behavior by pre-identified dominant market participants.

(3) Extension of Consent Decree or permanent task force to bring faster antitrust action

The current supervising court in Microsoft should give consideration to the extension and expansion of Consent Decree to monitor more than just openness and licensing of APIs. Expansion of oversight into security software and other software marketplaces should be considered. Predatory conduct should be spotted and prevented early before software monoculture in certain key software markets can be accomplished by certain large market share players like Microsoft.

b) Market dominant players must be countered with more rapid examination and perhaps litigation if they attempt predatory actions.

In conclusion, consideration of what could be done to more rapidly counter violations of the Sherman acts by certain pre-identified market participants. It should be remembered that the Microsoft court retained the jurisdiction to enforce the Consent Decree on its own volition without prompting from the government or Microsoft [112].

II. Antitrust enforcement isn't keeping pace with the pace of marketplace challenge

This author and others [113], while concerned that the slow pace of antitrust enforcement is no match for the pace which monopolists can abuse their marketplace power to harm consumers, believed that antitrust has a place in promoting competition in the consumer software marketplace.

A. Antitrust law is relevant in the "New-Economy" but reform is needed

As antitrust Professor David Evans observes, "The basic principles of antitrust apply just as well to the New Economy as to the old. Agreements to fix prices or to restrict output are surly as bad in the information age as they were when John D. Rockefeller was making it almost impossible for rivals to move oil to market"[114]. That being said, justice delayed is justice denied. As Chief Justice Burger has noted: "A sense of confidence in the courts is essential to maintain the fabric of ordered liberty for a free people and three things could destroy that confidence and do incalculable damage to society: that people come to believe that inefficiency and delay will drain even a just judgment of its value; that people who have long been exploited in the smaller transactions of daily life come to believe that courts cannot vindicate their legal rights from fraud and over-reaching; that people come to believe the law - in the larger sense - cannot fulfill its primary function to protect them and their families in their homes, at their work, and on the public streets" [115]. Antitrust enforcement can only remain relevant to the New Economy if there is some commitment that antitrust enforcement will evolve to meet the challenges of New Economy businesses. The true clients of antitrust are consumers. If consumers are being injured at an unprecedented by actions which can and do unfold at never before

experienced pace then antitrust enforcement mechanisms have to be developed to act more rapidly and proactively.

B. Lawmakers must move to address the chasm that exists the speed which market dominant players exploit their power to tip software applications spaces in their favor excluding alternative solutions and the speed which antitrust authorities act

More forward looking approach is necessary. This fact is starting to become apparent [116] but there is of course a discomfort with courts imposing regulatory injunctions that involve detailed governmental supervision of firms [117]. More proactive monitoring of certain conduct has arguably got to be added to present conduct. Identification of key product areas where competition needs to be actively monitored and Strict scrutiny of MS activities maintained.

C. Key points – Will there be effective reform in the future

- **Antitrust modernization efforts need to recognize the pace of enforcement problem**
- **Antitrust modernization efforts need to recognize the danger of looking backward and not proactively forward**
- **Current enforcement cases like Microsoft could benefit from market behavioral trip-wires. Automatic review of certain actions by high market-share participants in software markets for certain critical applications markets?**

Conclusion:

As noted early Antitrust law has a part to play in the new economy but ways have got to be found to synchronize its power against the conduct which it was designed to regulate. Waiting until damage is done and then finding fault after it's too late to prevent the market disruption just doesn't fit with the rapidity that the market moves and at which severe damage can be done to the innovation and competitive process. Business moves in real time, some way has got to be found to accelerate monitoring of those players like Microsoft and Google who are the most likely suspects to engage in behavior proscribed by the Clayton and Sherman acts.

Some attempts have been made to modernize antitrust enforcement to no avail. We would argue that it is time to take a new look at a régime that would bring more routine scrutiny of the repeat offenders and set proactive tripwires. These tripwires might not trigger automatic litigation but they should ensure that certain activities like zero dollar pricing for software by monopoly players or market share movement towards monoculture in certain key software markets is mandatorily analyzed and referred immediately to the Antitrust division.

With huge the natural monopolies that have formed in the technology sector, clarity of conduct and agility in enforcement have never been more critical. Given major corporations have the ability to put companies, such as security software suppliers, that are central to the security of our nation, with a single click, understanding and evolving anti-trust enforcement to meet the challenge of a new age economy has never been more important.

1. (Findings of Fact, U.S. v. Microsoft Corp., Civil Action No. 98-1232 (TPJ) and State of New York, ex rel, et al. v Microsoft Corporation, November 5, 1999)

2. (U.S. v. Microsoft Corp., Civil Action No. 98-1232 (TPJ) and State of New York, ex rel, et al. v Microsoft Corporation, (D.D.C. November 5, 1999))

3. Software as a Service (SaaS, typically pronounced 'sass') is a model of software deployment whereby a provider licenses an application to customers for use as a service on demand. SaaS software vendors may host the application on their own web servers or download the application to the consumer device, disabling it after use or after the on-demand contract expires. The on-demand function may be handled internally to share licenses within a firm or by a third-party application service provider (ASP) sharing licenses between firms (Wikipedia: Software as a service (SaaS))

4. (Findings of Fact, U.S. v. Microsoft Civil Action No. 98-1232 (TPJ) (D.D.C. 1999))

5. For more about the history of the Netscape Browser as a product *see* http://en.wikipedia.org/wiki/Netscape_Browser

6. Charlie Rose, Interview with Marc Andreessen, PBS October 16, 1996 available at http://www.charlierose.com/view/interview/ 5908. Netscape senior vice president of technology and co-founder Marc Andreessen shares his story of developing the prototype for the first Netscape browser on the Internet while still a college student and then the process of transforming it into the Netscape Navigator. Netscape is used by over 40 million people and is a head-to-head competitor of the Microsoft Corporation.

7. See http://money.cnn.com/1998/11/24/technology/aol/. "AOL, "Netscape tie knot" CNNfn November 24, 1998: 3:47 p.m. ET. "Link with Sun Micro formed; $4.2B deal seen challenging Microsoft.

8. Netscape's share of U.S. browser use was above 80 percent throughout most of 1996. This figure is based on both internal tabulations maintained by Netscape, which were obtained as part of the discovery process, the tabulations from the University of Illinois site later cited by the government. See Transcript in U.S. v. Microsoft Corp., Civil Action No. 98-1232 (TPJ).

9. (Internet World Statistics)

10. (Internet Usage Statistics)

11. (Cho) at v.

12. (Cho) at v. See (Cho) at Chapter 2, 5-40, generally for worldwide antitrust enforcement actions against Microsoft.

13. In addition to actions against Microsoft by the U.S. Federal Trade Commission ("FTC") and the United States Department of Justice Antitrust Division ("DOJ") there have been numerous actions brought for a variety of anti-competitive behavior by individual U.S. States. See (Cho) at 27-28.

14. See (Cho) at 40-112 for an in-depth analysis for the action against Microsoft in Korea, a key market for PC software distribution.

15. (Cho) at 21.

16. U.S. v. Microsoft Corp., Civil Action No. 98-1232 (TPJ) (U.S. District Court for the District of Columbia)

17. (W. H. Page) at 129.

18. (W. H. Page) at 131.

19. (Shapiro) at 761.

20. (W. H. Page) at 132-134.

21. Paraphrasing (Eliot)

22. (Sowell). "Five years is breakneck speed for completion of a major antitrust case and it is not unknown for a decade or more to elapse before the appellate courts

say the last word on one of these cases. Five years is at least two generations when it comes to computers. A decade ago, laptops were a novelty of the rich."

23. (Posner, Antitrust Law, Second Edition) at 286.

24. (Posner, Antitrust Law, Second Edition)at 286.

25. (Posner, Antitrust Law, Second Edition) at 282.

26. (Posner, Antitrust Law, Second Edition) at 282.

27. IBM was mired in antitrust litigation for thirteen years in the 1980s. (Konrad).

28. (Baker) at 1also found at http://www.brookings.edu/articles/2001/winter_regulation_baker.aspx.

29. (Carlton, Does Antitrust Need to be Modernized: Economic Analysis Group Discussion Paper)

30. (Klein, Statement of Joil I. Klein, Assistant Attorney General Antitrust Division, U.S. Department of Justice before the Committe on the Judiciary United States House of Representatives)

31. (Taft, DOJ's Klein Says Antitrust Critical In New Economy)

32. See Perspective: Diversity within crops restricts disease http://www.new-ag.info/01-1/perspect.html (Wolfe)

33. http://en.wikipedia.org/wiki/Crop_diversity. (Wikipedia entry: Crop Diversity)

34. (Geer, Bace and others) at 4.

35. (Iansiti) at 706.

36. Daniel Geer, Rebecca Bace, and others, "Cyberinsecurity: The cost of Monopoly; How the Dominance of Microsoft's Products Poses a Risk to Security." (2003). Computer & Communications Industry Associations General Meeting – Paper presented. Page 4. (Geer, Bace and others)

37. (Network Effect)

38. (Cho) Page 16. See also (Network Effect - Wikipedia, the free encyclopedia)

39. (Network Effect - Wikipedia, the free encyclopedia)

40. (U.S. District Court for the District of Columbia). The court stating in its finding of fact: '39. Consumer demand for Windows enjoys positive network effects. A positive network effect is a phenomenon by which the attractiveness of a product increases with the number of people using it. The fact that there is a multitude of people using Windows makes the product more attractive to consumers. The large installed base attracts corporate customers who want to use an operating system that new employees are already likely to know how to use, and it attracts academic consumers who want to use software that will allow them to share files easily with colleagues at other institutions. The main reason that demand for Windows experiences positive network effects, however, is that the size of Windows' installed base impels ISVs to write applications first and foremost to Windows, thereby ensuring a large body of applications from which consumers can choose. The large body of applications thus reinforces demand for Windows, augmenting Microsoft's dominant position and thereby perpetuating ISV incentives to write applications principally for Windows. This self-reinforcing cycle is often referred to as a "positive feedback loop." '

41. (Network Effect - Wikipedia, the free encyclopedia). See also (Cho) at 16.

42. See (Cho) at 17.

43. (Cho) at 18.

44. (Rubinfeld)

45. See for example (Clark)

46. (Posner, Antitrust Law, Second Edition) at 255.

47. (Posner, Antitrust Law, Second Edition) at 255.

48. See generally (Posner, Antitrust Law, Second Edition) at 256.

49. See (Economides)for a economics oriented discussion of predation: "The traditional [economic] theory of predation requires that a product be sold below incremental (or "avoidable") cost for a period of time until competitors are driven out of business; then the monopolist increases prices and reaps its monopoly profit. See e.g. (Areeda and Kaplow) at 512, 514.

50. The "Fisher Rule." Discussed at length see (Economides, The Microsoft Antitrust Case: Rejoinder). Formulated by Dr. Fisher in testimony in

51. (United States v. Microsoft)

52. [1]See (Brooke Group Ltd. v. Brown & Williamson Tobacco Corp.) available at http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=509&invol=209

53. (Fisher)

54. (Brooke Group Ltd. v. Brown & Williamson Tobacco Corp.) at 510.

55. (Findings of Facts, United States v. Microsoft (hereinafter "FOF")). See also (Microsoft III). See Microsoft II 84 F. Supp 2d at 111. (paragraph 408 discussing the effect on consumers of Microsoft efforts to protect the applications barrier to entry). See also (Economides) for a full discussion of the economic issues presented to the trial court and general criticism of the economic underpinning.

56. See (Cho) at 145.

57. (Cho) at 145.

58. (Clark) Security software: Microsoft accused of predatory pricing: http://www.channelregister.co.uk/2006/06/22/microsoft_predatory_pricing/

59. (Evers) Europe fears Microsoft's security push: http://news.zdnet.co.uk/security/0,1000000189,39283736,00.htm

60. Daniel Geer, Rebecca Bace, and others, "Cyberinsecurity: The cost of Monopoly; How the Dominance of Microsoft's Products Poses a Risk to Security." (2003). Computer &Communications Industry Associations General Meeting – Paper presented. Page 4.

61. (Wikipedia entry: George Santayana http://en.wikipedia.org/wiki/George_Santayana)

62. (Santayana). **George Santayana** (December 16, 1863, Madrid, Spain – September 26, 1952, Rome, Italy), was a philosopher, essayist, poet, and novelist. A lifelong Spanish citizen, Santayana was raised and educated in the United States, wrote in English and is generally considered an American man of letters. Of his nearly 89 years, he spent 39 in the U.S. Santayana is perhaps best known as an aphorist, most famously for his oft-misquoted remark "Those who cannot remember the past are condemned to repeat it," (sometimes called Santayana's Law of Repetitive *Consequences*).

63. *See* Cyberinsecurity: The cost of Monopoly; How the Dominance of Microsoft's Products Poses a Risk to Security. (2003). Computer &Communications Industry Associations General Meeting – Paper presented.

64. ibid

65. Jack Goldsmith, Defend America One Laptop at a Time. New York Times, July 1, 2009. http://www.nytimes.com/2009/07/02/opinion/02goldsmith.html

66. President Barack Obama, "Remarks By The President On Securing Our Nation'scyber Infrastructure." May 29, 2009. Press Release The White House Office of the Press Secretary.

67. See (Clark)saying, "According to [Sunware Software President Alex] Eckelberry, word processors, spreadsheets and browsers don't threaten the safety of users or the national computing infrastructure as much as being forced to buy your security software from the same company that also makes your applications and operating systems. In a world where Microsoft has a hegemony on security, he warns. 'the implications may be far reaching, *possibly to our own national security"*'

68. (Geer, Bace and others) at 11.

69. (Mahinka) at 124.

70. See (Cho) at 18. See also (Network Effect - Wikipedia, the free encyclopedia). See (Sheehan) for discussion *The Browser Wars: 2009, a Tipping Point for Microsoft?*

71. (Goodwin). *Google calls for court to tighten Microsoft's anti-trust leash: Doesn't trust Microsoft to supervise itself*

72. (Romano). *Microsoft will change Vista desktop search after complaint by Google*

73. (Geer, Bace and others) at 13.

74. (Ohlausen) at 691. The U.S. Department of Justice Antitrust Division web site provides links to all the federal court filings and decisions associated with the Microsoft antitrust challenges at http://www.usdoj.gov/atr/cases/ms_index.htm.

75. (Elzinga, Evans and Nichols) at 129-131

76. (United States v. Microsoft Corp., Civil Action No. 94-1564 (SS)(D.D.C. 1994))

77. The U.S. Department of Justice Antitrust division sued Microsoft on July 15, 1994 alleging violations of 15 U.S.C. §2 ("§2 of the Sherman Antitrust Act") complaining that Microsoft had entered into licensing agreements with computer Original Equipment Manufacturers ("OEMs") that prevented other operating system vendors from gaining widespread distribution of their products.

78. (Consent Decree, U.S. v. Microsoft Corp., Civil Action No. 94-1564 (SS), (D.D.C. August 21, 1995)) hereinafter "The 1995 Consent Decree."

79. (15 U.S.C. §2)

80. The main accusations in United States v. Microsoft were:

81. Monopolization of the market for operating systems ("OSs") for Personal Computers ("PCs" through the use of anti-competitive contractual arrangements with various vendors of related goods such as software developers, Internet Service Providers ("ISPs") and Internet content providers and of other actions taken to preserve and enhance its monopoly, and that these acts are illegal under §2 of the Sherman Act;

82. Attempting to monopolize the market for Internet browsers which is illegal under §2 of the Sherman Act;

83. Anti-competitive bundling of the Internet Explorer ("IE", the Microsoft Internet browser, with the Windows operating systems, which is illegal under §1 of the Sherman Act. See also (Economides, United States v. Microsoft: A Failure of Antitrust in the New Economy) for a good history of the Microsoft III Case.

84. (Complaint, United States v. Microsoft Corp., No. 98-1232 (D.D.C. 1998)); (New York v. Microsoft Corp., Case No. 98-1233, (D.D.C.) 1998) The state and federal suits were filed separately, and later consolidated, (United States v. Microsoft, 253 F.3d at 47 (D.D.C. 1999)), but diverged again in the remedies phase, (United States v. Microsoft States Remedy, 224 F. Supp. 2d at 87 (D.D.C) 2001)

85. (15 U.S.C. §1)

86. (U.S. v. Microsoft Corp., 84 F. Supp. 2d 9 (D.D.C 1999)) [hereinafter *D.D.C. Findings* 1999].

87. (U.S. v. Microsoft Corp., 84 F. Supp. 2d 9 (D.D.C 1999)) at 15-19. The court found that Microsoft's market share for PC operating systems was above ninety percent.

88. See (Network Effect - Wikipedia, the free encyclopedia) and discussion infra for a description of "Network Effect".

89. The "applications barrier to entry" played a central role in the U.S. Department of Justice's and state plaintiffs' theory of their consolidated case against Microsoft. See e.g. for a excellent description of the importance of the "applications barrier to entry in earlier litigation: (New York v. Microsoft Corp., 531 F. Supp. 2d 141 (D.D.C. 2008).) (U.S. v. Microsoft Corp., 84 F. Supp. 2d 9 (D.D.C 1999)) at18-24. A good discussion of issues of market definition in Microsoft can be found in (Page and Lopatka, The Microsoft Case: Antitrust, High Technology and Consumer Welfare). This source at pages 203-42 offers a good tabulation of the court, date and a citation of the volume and page number of the multitude of opinions by various courts in the Microsoft litigation.

90. Applications Barrier of Entry plays a key part in the case against Microsoft's actions to preserve its hegemony in PC Operating systems, see (Competitive Impact Statement) Competitive Impact Statement, United States v. Microsoft Corp., No. 98-1232 (D.D.C. Nov. 15 2001) at 17.

91. Applications Barrier of Entry: As an operating system gains new users its existing users befit because developers will have an incentive to write more application programs that rely on the operating system's interfaces and Applications Programming Interfaces ("API's"). For more discussion of APIs see (McKenzie) *Microsoft's "Applications Barrier to Entry": The Missing 70,000 Programs.*

92. (Plaintiff's joint proposed findings of fact in Microsoft 84 F. Supp. 2d 9 (D.D.C 1999) Microsoft has engaged in a broad pattern of unlawful conduct with the purpose and effect of thwarting emerging threats to its powerful and well-entrenched OS). See

also (Rudolf Peritz) at 324 for a discussion of “middleware” and its threat to the dominance of the Microsoft Windows OS.

93. (Findings of the Court, United States v. Microsoft 84 F. Supp. 2d at 20 (D.D.C. 1998))

94. (Economides, United States v. Microsoft: A Failure of Antitrust in the New Economy) at 8. See also (Auletta)

95. The hearing held May 24, 200 started at 10:15 am and ended about 3:30pm including a two hour lunch break.

96. See generally (New York Times April 2, 2000)

97. See generally (Elzinga, Evans and Nichols)at 142-146.

98. (U.S. v. Microsoft Corp., 87 F. Supp. 2d 30, 45-46 (D.D.C. 2000) [hereinafter D.D.C. Conclusions 2000]). See generally (Cho) at 23.

99. (D.D.C. Conclusions 2000) at 33-45

100. (D.D.C. Conclusions 2000)

101. (D.D.C. Conclusions 2000) at 80

102. (D.D.C. Conclusions 2000) at 105-107

103. (U.S. v. Microsoft, 253 F3d at 116-17 (2001 D.C. Circuit))

104. Illinois, Kentucky, Louisiana, Maryland, Michigan, New York, North Carolina, Ohio, and Wisconsin. See (Competitive Impact Statement, U.S. v. Microsoft Corp. Div. No. 98-1234 (D.D.C. Nov. 15, 2001))

105. (Proposed Final Judgement U.S. v. Microsoft Case No. 98-1232 (D.D.C. 2001))

106. (D.D.C. States Remedy 224 F. Supp. 2d (2002) [herinafter the 2001 Consent Decree])

107. See generally (W. H. Page) for a full history and description of the settlement scheme laid out in the final 2001 Consent Decree.

108. (Final Judgement Purshuant to Rule 54b, U.S. v Microsoft Corp., Case No. 98-1232 (CKK) and No. 98-1233 (CKK) (D.D.C 2002)).

109. (W. H. Page) at 129.

110. (W. H. Page) at 131.

111. (Shapiro) at 761.

112. First and Gavil)at 644.

113. (W. H. Page) at 132-134.

114. Paraphrasing (Eliot)

115. (Ohlausen) at 701.

116. See (Evans, Microsoft, Antitrust and the New Economy)

117. (Evans, Microsoft, Antitrust and the New Economy) at 262.