Comments of Jay Sulzberger to the FTC in regard to issues raised at the FTC P2P File Sharing Workshop, 15-16 December 2004.

Plan of my comments.

My name is Jay Sulzberger. Below are my comments on issues examined at the FTC P2P File Sharing Workshop of 15 and 16 December 2004. I do not closely answer the formal questions posed by the FTC because I believe that some clarification of terms and some exposition, and some correction, of assumptions is required in order to lay a foundation for detailed analysis of actual abuses. I believe some of these abuses may be effectively addressed by FTC action.

There are two meanings of the words "peer to peer network" and we should not confuse them.

From http://www.ftc.gov/os/2004/10/041015p2pfrn.pdf:

The FTC's workshop, "Peer-to-Peer File-Sharing Technology:
Consumer Protection and Competition Issues," will continue the Commission's long-standing efforts to assess the impact on consumers and businesses of new and significant technologies, such as peer-to-peer (P2P) file-sharing technology. P2P file-sharing technology provides individuals with the ability to share files, including music, video, or software files, with other users. The files do not reside in a central location, but rather are stored on the hard drives of the users of the software. [see note 1] Users download particular file-sharing software that gives the user access to selected files on the computer hard drives of other users on the same P2P file-sharing network. Users may also place files that they have labeled into a shared folder on their hard drive, thereby making these files available for sharing with users of the same network. By eliminating the need for a central storage point for files, P2P file-sharing technology allows for faster file transfers and conservation of bandwidth.

There are two meanings to the words "peer-to-peer (P2P) file-sharing network". The first, original, and primary meaning is the Net we have today, as envisioned by Licklider at ARPA in the early Sixties of the Twentieth Century. A new, secondary, and misleading meaning is the small number of widely used systems for swift indexing, presentation of the catalog, and distribution of, mainly, popular songs. Some of the songs are under standard mass market restrictive copyright rules, others lie in the public domain, and some are licensed under less restrictive copyright rules. The details of the flow of bits, packets, data, and meta-data are less important than the breathless and seemingly endless articles on the "P2P phenomenon" assume/imply/declaim; there are many private and public and part-private part-public networks, with various patterns of bit-flows, built on the Net, e.g., Akamai, CPAN, DNS, DoubleClick, mailing lists, various VPNs, the recent un-designed net and sub-nets of blogs, and more. We who have used the net for decades know that the net is a peer to peer network. My computer can transmit and receive information, that is, files, to and from your computer, without

dealing with any third party, at the levels of law or money or custom. This is the original meaning of "peer to peer". That some people, for love or money, have built and published software, riding atop the Great Peer to Peer Net, which makes the collection and distribution of the Bootylicious works of Destiny's Child, and other music, particularly easy, is not surprising, and it is not new. Usenet meets the most stringent criteria which define the small set of applications now called peer to peer, and Usenet was, if memory serves, up and running by 1980.

A question which the FTC almost explicitly poses.

I shall not address your questions individually, but rather I will attempt a general answer to the question

"How come so many home machines are so badly infested by parasite programs?"

This question is the right question to ask, because in this form it allows of better answers, which suggest better remedies. Asking whether P2P applications [new terminology] are a better substrate for worms, viruses, key-loggers, etc. than http daemons and browsers as commonly used five years ago, frames the question too narrowly, and imposes a statistically incorrect and legally labile distinction. The right partition lies at the level of the OS, and at the level of law and custom and culture. Today if you run a source secret OS, such as any of the recent Microsoft OSes, you have almost no practical control over what is running on your hardware, and legally and economically, no recourse, so long as you run the incompetent OS. By an odd interpretation of copyright law, you are not legally permitted to seek effective repairs of your OS. Thus there is no market in effective repairs of Microsoft's defective product. Certainly many companies sell partial and inadequate remedies in the forms of "anti-virus", "firewall", "ad-blocker", etc. software. These companies enjoy the advantage that their products never succeed at their tasks; you will always need to update the after-the-mass-infestations lists of virus fingerprints, and every add-on firewall is soon defeated by the traditional cooperation of worm writers and Microsoft's reliable team of devil may care designers and coders. Yet for computer sophisticates there is an effective remedy. On low cost IBM personal computer style hardware, you may today run a free operating system, such as GNU/Linux, or one of the free BSDs. In practice, among those who run such free operating systems, the rate of infestation is significantly lower, certainly a factor of one hundred times lower, than among those who run Microsoft OSes. In addition we spend much less time fiddling trying to harden our systems. Many distributions, such as Knoppix, a variant of Debian GNU/Linux, are decently defended out of the box. There are two reasons our systems are better than Microsoft's source secret systems:

1. The design of Microsoft's OSes is less good than the design of today's free Unices. Our execution is better too.

2. We know we can own our own computers. We know we can get practical control of our systems. We know that if a problem arises we can, with complete probity, and without legal trammels,

a. attempt a fix on our own lonesome
b. ask friends in private to help
c. ask for help in public at meetings and on mailing lists and web sites of individuals and tribes of the Free Software Nation
d. buy a solution already developed
e. pay for development of a solution

The design incompetence of 1 could be corrected by Microsoft, but has not been for years. But no vendor of a source secret OS can offer the home user full use of the powers enumerated in 2. These freely exercisable powers, of course, are just the beginning of the benefits that a larger and more free market in OSes provides. We know the productive power of free software: we have more than one OS stack, and we are steadily improving what we have produced over the past twenty years, and we are now starting to build completely new systems, which will offer yet further increments of ease and power and delight.

The root cause of the plagues of parasites suffered by millions of home users today is that most buyers of home computers do not know that they have a choice of operating systems. The distinction between "P2P" and "server client" is evanescent and unclear (what level of transport of data and meta-data are we talking about, on what time scale), while the distinction between an OS stack which is transparent to many thousands of eyes, and an OS stack which is legally a black box, is the relevant distinction here. If the OS is transparent, as the GNU/Linux, and the FreeBSD, NetBSD, and OpenBSD systems are, then there is some hope of effective remedies using regulatory, statute, and common law, and a more free market, and tribal cooperation. If the OS is source secret, it is, by design, not transparent, and there is no affordable legal means of forcing the vendor to give practical powers of control to the home user, and certainly, there can be no legal market in repaired, or improved, versions of the OS, nor can voluntary non-profit associations openly cooperate to improve the position of the home user.

The grave danger of an attempt at special regulation of "P2P networks" is that such regulation result in a system of government management of every part of the net, from the lowest level protocols to the highest levels of user-machine interfaces. Because of the lack of a stable principled distinction between "P2P" and the Net itself, it is likely, if "P2P regulations" be imposed, that the threat of litigation and/or police intrusion would attend the publication of even the smallest shell script that calls any net service, such as http transport, ftp, rsync, ssh, net sockets, etc.. The difficulty of legally circumscribing a class of "P2P" applications distinct from the Net itself and the large class of Net applications, is demonstrated by Professor Ed Felten's small program tinyp2p. tinyp2p is a working "P2P" application whose source code consists of less than a screenful of Python code. tinyp2p is at http://www.freedom-to-tinker.com/tinyp2p.html

Note that most Net infrastructure software is free software, and that the standard Python programming system is free software, and the Python system is compiled using gcc, the GNU C compiler, which is also free software. Of course, the much used "P2P"

application BitTorrent is also free software. Note that neither tinyp2p nor BitTorrent were built by any for profit entity, nor do the authors of these "P2P" applications derive any income when you or I or one million people use their work. Nor can the authors restrict your or my or one million people's use of these Net applications. It is hard to conceive of any regulations or laws that would suppress the production, distribution, and use of such Net applications, without gross abrogation of our present legal rights of copyright, private ownership of computers, and freedom of speech and association.

How is it possible that so many people are unclear that they have a legal right of ownership, and some possibility of practical control, of the computer system they paid for?

It is because for over a decade Microsoft operating systems have been, for most buyers of low cost home and office computers, the only operating systems available. At point of sale, low cost computers can only be purchased with Microsoft operating systems already installed. Indeed, at J and R's big computer and home electronics store near City Hall in New York City, a smooth wall of Microsoft OSes greets the prospective buyer of any low priced computer system. No other OSes are offered at point of sale of the hardware, and no hardware is offered without an already installed Microsoft OS bundled in.

Now most owners of home computers are not computer experts. Nor are most reporters who write stories on computers, not even reporters for large circulation newspapers. Most owners of home computers are not aware that their hardware is capable of running other operating systems than Microsoft's. Indeed most do not clearly understand the distinction between the hardware and the OS.

To repeat: Microsoft's OSes are under a restrictive copyright license which is interpreted to make illegal both discovery and publication of exactly what the Microsoft OS is doing. This legally enforced market deformation is the fundamental cause of the plague of parasites.

This situation obtains not because "end users choose Microsoft", but because a large scale and long running combination in restraint of trade has been entered into by Microsoft, Dell, CompUSA, IBM, and most big vendors of low cost computers.

The fundamental agreement of this broad cartel level action to deny most buyers a choice of operating systems is that no OSes, except Microsoft's, may be installed, or even mentioned, at point of sale of the hardware. Further, despite the famous Refund Clause of the Microsoft End User License Agreement, any attempt to obtain a refund on the Microsoft OS is refused by joint action of Microsoft and the hardware vendor.

We call the attention of the FTC to the remarkable crudity of both the illegal general agreement to force Microsoft OSes on buyers, and the further contumacious attempts to deny any buyer of the hardware, no matter whether or not the buyer has met the requirements for a refund, from getting their refund.

These illegal agreements are neither denied nor disguised by the hardware vendors. If you ask Dell whether they will ship you a home computer without any Microsoft OS, their employees inform you, with complete nonchalance, that they have an agreement with Microsoft to never ship any computer without a Microsoft OS; should you inquire as to whether Dell will honor the Refund Clause, you are blandly informed that Dell will, under no circumstances, ever honor the Refund Clause, and if you ask Microsoft, whose EULA it is, Microsoft refers you to Dell for an answer.

But we have yet to answer our question: "Why is this bad situation so nearly universally not understood?". Here is the answer. Most people believe that the problems of Microsoft's incompetent and insecure OSes are necessary failures of every possible OS, because Microsoft and the hardware vendors have succeeded in concealing the existence of other OSes. This mistaken, and mostly implicit, belief is well supported by most large circulation news sources, simply because reporters and management share the belief.

This erroneous proposition is seldom cleanly expressed, since most who hold this belief also do not know what an OS is, much less that there is more than one for their hardware. Naturally this makes bringing evidence against the false assumption harder, since one has to first bring the holders of the false assumption to a statement coherent enough to be denied.

What should the FTC not do?

The FTC should not attempt any direct regulation of "P2P", new sense, as such. Any such regulation must, because of the radical lack of distinction between "P2P" applications and the Net, in principle be a general regulation of our computers and our Net.

The FTC should not impose any regulations arrived at by agreement between lobbying groups for "P2P" and the government, on the further particular ground that such regulation would erect barriers to entry into the field of Internet Applications to the unfair benefit of present companies, and the detriment of nascent for profit and non-profit systems which make use of the Net.

What should the FTC do?

Minimally burdensome enforcement of common rules of contract, consumer protection, and anti-trust, will accomplish much to reduce all the risks asked about in the FTC's call for response.

In particular, the FTC should take action to cause Microsoft and hardware vendors to honor the Refund Clause of the Microsoft EULA. Bill Gates and I agree that such action would quickly result in many people running more competent free OSes. Such action toward enforcement of the EULA lies squarely within the ambit of the FTC, and would

not infringe in any way on my freedom to publish shell scripts, cooperate in improving free OSes, etc..

Property rights and freedom of speech are delicate things.

The FTC can do some things to help home users understand that they can gain legal and practical control over the computers in their houses. But the FTC in its actions must strike at the right level, else the remedy will be worse than the disease.

We are fortunate in the structure of the parasite problem: The most dangerous proposed actions, such as direct regulation of "P2P" applications and companies and authors and users, are also the actions that would have the least effect on the problem of parasites. The most effective actions are also the least dangerous to our rights. Requiring Microsoft and the hardware vendors to adhere to the plain and simple and specific Refund Clause of the EULA, which EULA Microsoft wrote, is not a general regulation of the Net.

Thank you, FTC Commissioners!

Thank you for reading this!

I remain, as ever, your obedient servant, viewer with alarm, and citizen of the United States of America,

Jay Sulzberger working member of New Yorkers for Fair Use
http://www.nyfairuse.org