HOW TECHNOLOGY CAN HELP IN FIGHTING COUNTERFEITING AND PIRACY

David Finn
Associate General Counsel,
Worldwide Anti-Piracy and Anti-Counterfeiting
Microsoft Corporation

Third Global Congress on Combating Counterfeiting and Piracy
Geneva, 31 January 2007

Executive Summary

Intellectual-property counterfeiters and pirates increasingly use sophisticated technologies to break the law, which has caused the number of infringements to grow substantially. It is critical, therefore, that industry and government work together and use technology to cope with this unprecedented volume of piracy. The need for better and more widely used technology tools to speed up identification of infringing physical products and detection of online infringements will be highlighted.

Introduction

Counterfeiting and piracy are increasingly high-tech crimes. Their impact on society spreads even to computer damage and security breaches. It is only logical that high-tech solutions are needed for these high-tech crimes—to catch up with the criminals and to prevent and deter infringements.

There is a lot that the private sector and public authorities can do in cooperation with each other to modernize our enforcement tools and find, collect evidence, prosecute and stop infringements in smarter and faster ways.

I. Counterfeiting and piracy are a real economic and societal problem, which is increasing in scope and sophistication. A strong commitment from the government and private sector is necessary to address the problem.

A. Economic, employment, tax and innovation losses

We are all familiar with the economic and societal problems associated with counterfeiting and piracy—lost legitimate sales, lost taxes, lost jobs, and a lost return on investment that otherwise would be funding creative and innovative activity of benefit to all of society.

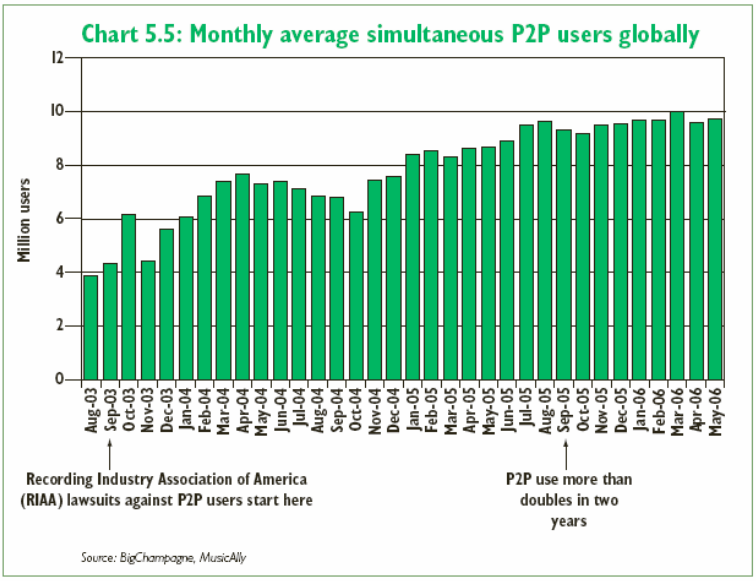
In the business software area, this loss and damage is staggering:[1]

35%	Average business software piracy rate worldwide;
$34.3bn	Worldwide piracy losses for business software;
2.4mn	New jobs that would be created if piracy rates dropped by 10%;
$70bn	New tax revenues that would be raised if piracy rates dropped by 10%;
$400bn	Local GDP growth that would be realized if piracy rates dropped by 10%.

[1] IDC/BSA, Global Software Piracy Study (May 2006), http://www.bsa.org/globalstudy/upload/2005%20Piracy%20Study%20-%20Official%20Version.pdf; IDC/BSA, Expanding the Frontiers of our Digital Future: Reducing Software Piracy to Accelerate Global IT Benefits (Dec. 2005), http://www.bsa.org/idcstudy/pdfs/White_Paper.pdf.

B. **Increased risk and complexity of internet counterfeiting and piracy**

Particularly with the advent of the internet, the problems associated with counterfeiting and piracy have grown in scale, complexity and speed. Recent estimates have shown that nearly 10 million people are on peer-to-peer or so-called 'file sharing' networks worldwide at any one time.[2] This seems to be a large number, but it is a small number compared to the 1 billion internet users.



Peer-to-peer technology is a promising and positive technological development, of course, and consumers are now starting to see legitimate peer-to-peer music services offer a wide variety of products and price options. At the same time, however, the courts have quite properly addressed *illegal* uses of this technology that undermine the legal protections afforded to copyright owners.[3]

C. **Threat to IT security and systems integrity**

The increasing use of the internet and technology to carry out infringing activities raises some important new policy considerations that governments should care about in making the fight against counterfeiting and piracy a priority: IT security and systems integrity.

It turns out that not only do internet pirates offer infringing copyright material, counterfeit serial numbers, and tools for 'hacking' or 'cracking' protected works, they often include other bits of software that will damage your computer, breach system security, or spy on computer activity.

A new research study entitled *The Risks of Obtaining and Using Pirated Software,* which is published by the respected IT research group IDC, shows that pirate websites regularly pass along computer viruses, worms, Trojan horses, adware, spyware and other unwanted or harmful material with pirated items.

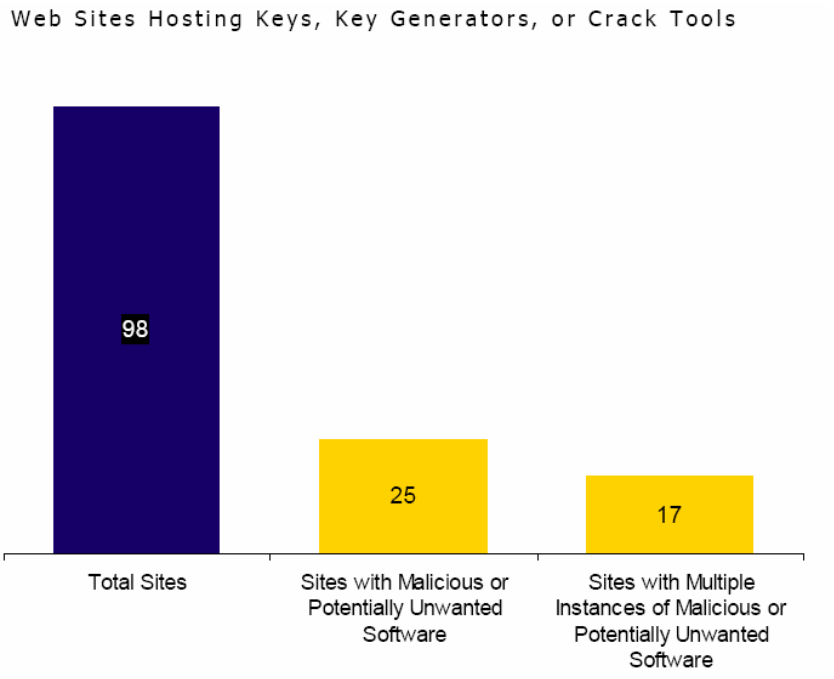
The IDC's research found that:

---

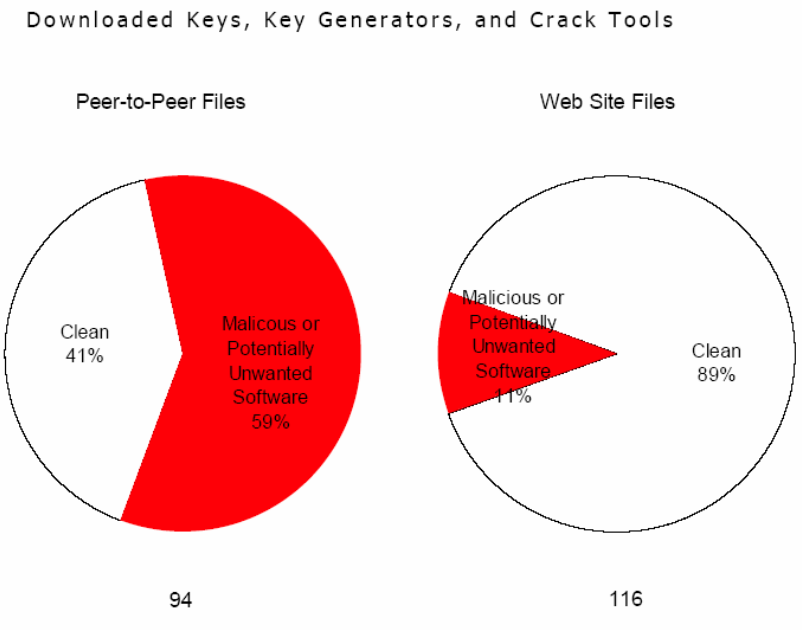
[2] Gowers Review of Intellectual Property, at 106 (Nov. 2006), http://www.hm-treasury.gov.uk/media/583/91/pbr06_gowers_report_755.pdf.

[3] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd*, [2005] FCA 1242 (5 Sept. 2005), *http://www.austlii.edu.au/au/cases/cth/federal_ct/2005/1242.html*.

25% of websites offering access to pirated software, counterfeit product keys and crack tools also attempt to install malicious or unwanted software on your computer.



59% of peer-to-peer downloads of counterfeit product-key generators and crack tools attempt to install malicious or unwanted software.[4]



.

[4] IDC, The Risks of Obtaining and Using Pirated Software (Oct. 2006), http://download.microsoft.com/download/7/6/9/769E42E0-68C4-4826-838B-0F801DB2EFC2/IDC%20White%20Paper%20on%20Risks%20of%20Pirated%20Software.pdf.

In September 2006, Microsoft also announced widescale forensic research into a sample of 348 counterfeit Windows XP discs acquired in 17 countries. Of these discs, **34%** would not install or run at all, and **43%** of the rest contained additional programs or binary code that was not part of the genuine Windows product. Taken together, this study showed that close to **two-thirds** of counterfeits found in these countries either do not work or have additional code that could expose the user and others to denial-of-service attacks, bypass of password protection or application memory corruption.

Piracy is not only bad for the economy, bad for creativity, and bad for innovation, it is also bad for computer and network security—on which so much of the modern economy and life increasingly depend.

D. New enforcement issues: how to set priorities given the increased scope and sophistication of criminal activities?

Now more than ever, strong commitments from both government enforcement bodies and the private sector are needed, if we are going to make any difference to the counterfeiting and piracy problem. The increasing scope, sophistication and volume of criminal activity in the area of counterfeiting and piracy, particularly in the internet age, is a real issue that must be grappled with if we are to target our investigations and prosecutions well, use our resources effectively, and actually make a difference.

This is not an issue unique to piracy, of course. Experts say that internet-based security attacks on computers and computer networks conducted by criminal organizations have doubled every year since 2004—they are entering into almost a new industrial phase! Last year, it took a team of 400 police officers to arrest a network of 80 copyright pirates operating in Brazil. It is not just that we have new menaces, but that we have a lot of them.[5]

II. Better technological forensic tools, and strong public-private partnerships, are vital to have a serious impact on the problem of physical counterfeiting and piracy.

A. CD/CD-ROM/DVD production: vast and diverse

One important, efficient and cost-effective way that we can build our capacity to fight piracy is through better technological forensic tools, which is the focus of this paper. High-tech crime needs high-tech solutions, both for online infringements and for traditional types of piracy.

Replication of physical discs is still a massive problem, with more than 1,033 optical disc plants and a 58.2 billion disc manufacturing capacity in more than 78 countries worldwide. Just to give an idea of the scale of the pirate manufacturing problem, the demand for legitimate CDs, CD-ROMs and DVDs is about 28.4 billion annually, which leaves an overcapacity of about 30 billion discs.

Industry statistics show that these plants are in fact producing 35.5 billion discs, not just the 28.4 billion of legitimate orders—this leaves about 7 billion discs not accounted for, many of which are going into the pirate and counterfeiting channels.[6]

---

[5] *E. Kaspersky : « Le problème n'est pas tant les nouvelles menaces de sécurité que leur nombre »,* 01Net (26 Dec. 2006), http://www.01net.com/editorial/336542/interview/e.-kaspersky-le-probleme-n-est-pas-tant-les-nouvelles-menaces-de-securite-que-leur-nombre-/.

[6] Source: International Federation of the Phonographic Industry, Understanding & Solutions.

1,033 optical disc plants in more than 78 countries have an annual capacity of 58.2 billion discs, only 28.4 billion of which is used for legitimate CD, CD-ROM and DVD orders.

Pirate plants not only produce large quantities of counterfeit Microsoft and other software discs, but also fake music CDs, infringing software game CD-ROMs, and counterfeit film DVDs.

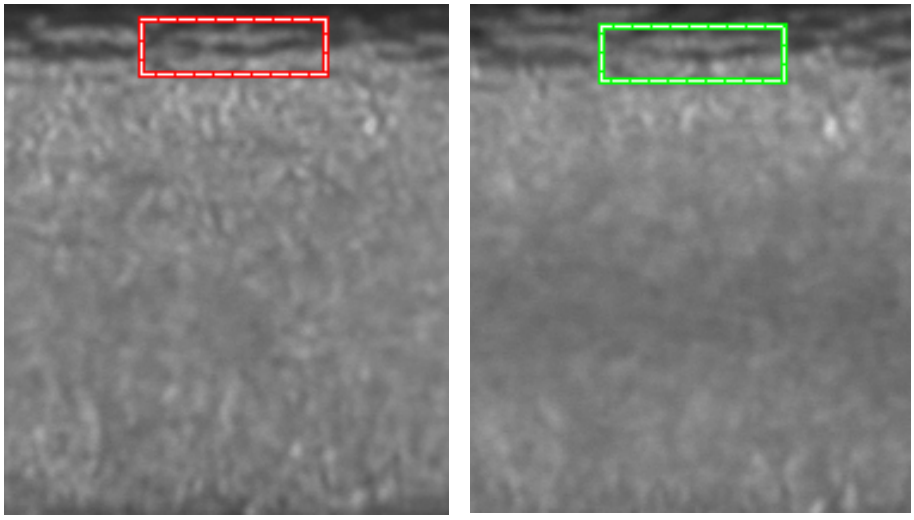
B. Traditional disc matching: manual and slow

Identifying the plants that have produced counterfeit CDs and DVDs is an incredibly efficient way to address counterfeiting, as it enables the investigators both to identify the counterfeiters who should be prosecuted and to cut off the source of infringing articles. Identifying the plants has other benefits: In international operations, it allows Customs to understand if products seized are coming from the same production sites as other material seized in other countries. It also can help identify the most prolific production lines in terms of products seized, or show links between different suspects that have been supplied by the same source.

But sorting through a mass of different discs found in a raid or a customs seizure, tracing them back to their production plant, and preparing this kind of evidence for a prosecution, can be a daunting task. Until now, both government enforcement authorities and the private sector have done this manually.

It is possible to track a counterfeit disc to a particular replication plant, by comparing the infinitesimally small grooves and patterns on that disc, known as 'micro mechanical striations', to those on an exemplar disc known to come from a particular plant. Each production line in a plant produces a unique set of such striations on all the discs produced on that line.

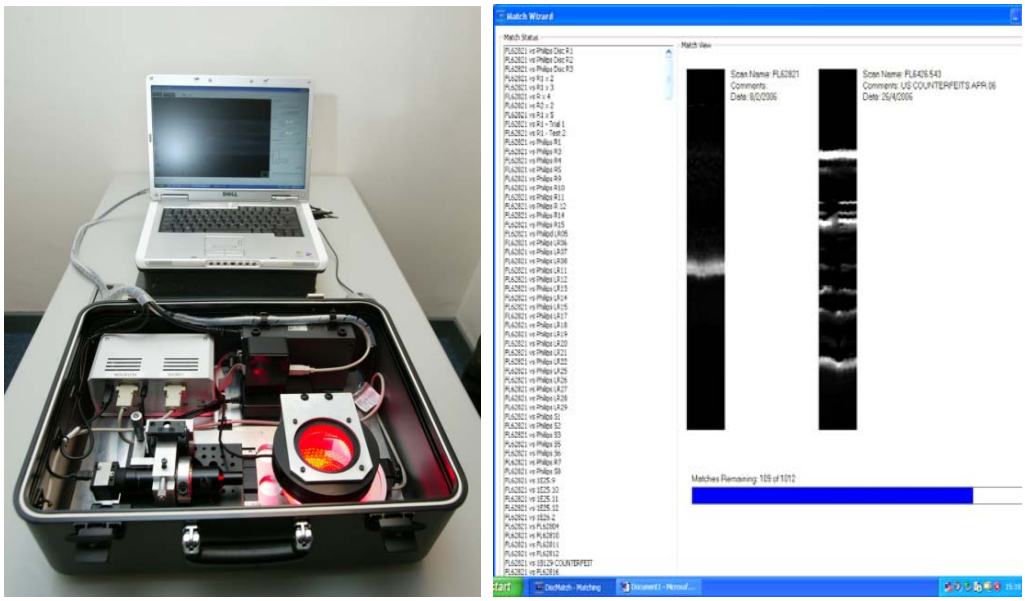
Traditional matching of unknown discs has been done on a microscope, and compared by a trained eye, disc by disc. These photographs show the kind of microscopic striations that must be compared to confirm a match. As you can imagine, this process is not terribly fast; a trained expert with access to the right equipment and exemplar database takes at least 10 minutes per disc.



Matching of the unique striations on counterfeit discs to exemplar discs from identified production plants can identify the source of pirate product.

C. **Opportunity to automate comparison of counterfeit discs with known exemplars**

One idea that Microsoft has been working on is a technology tool that would automate this forensic process for disc matching. We are calling this tool FRED, the Forensic Replication Exemplar Database. It's a PC based system that can be used to scan disc exemplars, create unique digital 'fingerprints' keyed to the unique striations of those exemplars, and then compare those known fingerprints to the fingerprints of counterfeit discs whose origin is unknown.



Disc matching system FRED can dramatically improve the speed and capacity of forensics on counterfeit discs.

The really useful thing about such a system is that it dramatically speeds up the disc forensics process. In our recent tests, we have found that a counterfeit disc can be checked using FRED against upwards of 200 known

exemplar discs per minute. The other advantage of course is that the number of investigators who could be doing disc matching, and the number of locations in which disc comparisons could be done, could be greatly expanded.

We are still testing FRED, but we are already talking with some stakeholders about how this kind of technology could be made widely available and used in partnership between public authorities and industry for the benefit of all.

III. High-technology detection, identification, and evidentiary tools also must be applied proactively to internet piracy.

A. Internet piracy, including peer-to-peer distribution, is the latest high-capacity source of pirated copyright material.

According to 2006 music-industry statistics, there are about 885 million infringing music files on the internet at any one time; most of these (775 million) are transmitted on peer-to-peer ('P2P'), so-called 'file sharing', networks, with another 100 million on pirate websites.[7] This is in fact *down* somewhat on the peak of 1.1 billion infringing music files on the internet as of April 2003, despite the nearly 40% growth of broadband penetration worldwide since that time.

The same trend has been noted in France. A study by GfK published by the French high-tech magazine SVM in January 2008 estimates that the number of files downloaded in France has fallen by 50% in one year, from 1.3 billion in 2005 to 620 million in 2006. More than 95% of these files are pirated. Only music has benefited from this reduction, according to the GfK study; movies and video games continue to be downloaded at the same pace. The total number of people downloading on P2P networks has continued to increase, from 4.4 million in 2005 to 5 million last year.[8] The reasons people give for their changes in behavior vary: On one hand, P2P users now tend to be more careful and selective, perhaps for fear of being caught; at the same time, half of the households still say they have no fear of being sued[9]. The security risks outlined by IDC in their study '*The Risks of Obtaining and Using Pirated Software*' probably play some role in people's thinking as well.

Software, games, films and other copyright material suffer similar unauthorized mass-distribution on the internet, and each industry is engaged in combating the problem using a range of different tools. Trade associations such as the BSA, of which Microsoft is a member, have engaged in a high-volume notice and takedown program, cooperating with internet service providers and internet auction sites to have infringements removed from the internet. Microsoft has also brought selected civil litigation and criminal enforcement cases against illegal internet offers of counterfeit products, pre-release downloads, and our trade secrets such as source code.[10]

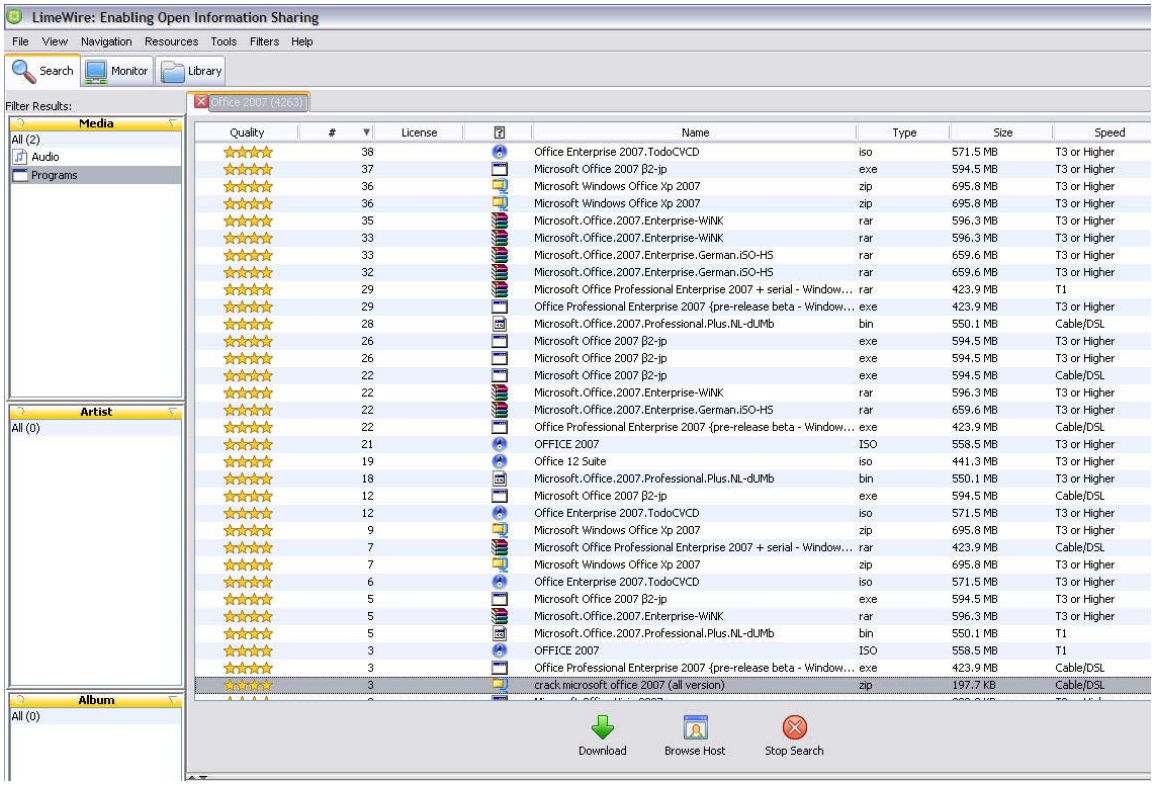
---

[7] IFPI, Digital Music Report, at 21 (2006), http://www.ifpi.org/content/library/digital-music-report-2006.pdf.

[8] http://www.svmlemag.fr/actu/sondage_exclusif_les_francais_misent_tout_sur_linternet (January 2007).

[9] http://www.zdnet.fr/actualites/internet/0,39020774,39366341,00.htm.

[10] *See, e.g.,* Business Software Alliance, *Consumers Duped by On-Line Pirates* (4 Oct. 2006), http://www.bsa.org/usa/press/newsreleases/Consumers-Duped.cfm; *Battle Against Software Pirates Intensifies,* Guardian Unlimited (31 Oct. 2006) , http://business.guardian.co.uk/story/0,,1936073,00.html; *U.S. man sentenced to two years in prison for selling Microsoft source code,* AP Worldstream (27 Jan. 2006), http://pqasb.pqarchiver.com/ap/892666671.html?did=892666671&FMT=ABS&FMTS=FT&date=Aug+30%2C+2005&author=&pub=Associated+Press&desc=Conn.+man+pleads+guilty+to+selling+Microsoft+source+code; Press Release, *Microsoft Intensifies Worldwide Campaign Against Internet Piracy and*



4,263 different infringing copies of Microsoft Office 2007, each offered numerous times, as well as cracking tools for the product, were available on this peer-to-peer service on 10 January 2007. This product has not yet been released for public distribution.

B. **Internet anti-piracy enforcement requires high-tech tools**

There are a number of forensic functions for which high-tech tools are needed in the fight against internet piracy. These include tools for:

- detection – *finding* offers of infringing copies of all kinds of content and other illegal material;
- identification - *identifying the lawbreakers*, which includes figuring out what service provider the infringer is using and obtaining the identification from that service provider—which usually requires a police or court process; and
- evidence gathering and analysis – *collecting and identifying information about the infringing material*, including the works in question, the quantities offered, dates and times and the like.

If you look across the various copyright-based industries and what they are doing on anti-piracy enforcement, the efforts to date have been rather piecemeal, with each group using its own vendors or technologies and very little coordination between each other or with law enforcement agencies. Microsoft itself relies on its trade associations' anti-piracy operations for a lot of this work, and does manual investigations or one-off use of third-party forensic suppliers for its most urgent cases.

Criminal Counterfeiting (2 Apr. 2001), http://www.microsoft.com/presspass/press/2001/apr01/04-02InternetCrimePR.mspx.

C. Internet anti-piracy enforcement could be more impactful through public/private partnerships

We do not have a good answer yet as to the best approach to internet piracy. ***Notice and takedowns***, and ***private-sector enforcement***, have their roles to play, of course. It is in fact the case that there are 'big fish' to be caught or prosecuted as a public example. NPD's analysis showed that 75% of all distribution of illegal music files on the internet was in fact done by 15% of the participating individuals.[11] So taking action against these 'big fish', whether via notice and takedowns or by private-sector enforcement, can act as a deterrent.

Sound high-tech tools are also a 'must' in conducting internet anti-piracy enforcement. The volume of infringements and the technical sophistication of some infringers are such that internet piracy is unlikely to be detected, traced or analyzed effectively without appropriate technology tools. But today's tools have inherent limitations, in that they tend to be used only by rights owner associations or their vendors and not by law enforcement itself. And some of the proposals suggested for future technologies—internet-wide filtering for example—have been simply unworkable for technology or cost reasons.

Law enforcement officials do need to take a proactive role in this area. The protection of intellectual property and its benefits for the local economies is an issue of interest for the whole society. Continued and visible actions by law enforcement agencies are one component of educating those engaged in piracy on the proper use of the internet, as well as the effects on society and risks to themselves that piracy brings.

Could public/private partnerships help governments build capacity to combat internet piracy, particularly by implementing more effective technology tools? We cannot say for certain, but this is something which we have already been asked for in another area—crimes against children. In January 2003, we received a request for support from the Canadian police to build a tool that would help them cope with the exponential volume of data involved in these types of cases. Working with the Federal Prosecution Service of Canada, we responded by developing the Child Exploitation Tracking System (CETS), a unique software tool developed by Canadian police, international law enforcement and Microsoft to help battle child exploitation online.

This tool helps law enforcement officials collaborate and share information with other police services based on legal agreements in place. CETS was created to increase the effectiveness of investigators and teams by providing them with software to store, search, share and analyze large volumes of evidence and match cases across police agencies. CETS has been deployed in Brazil, Canada, Indonesia, Italy, Spain and United Kingdom at the request of interested law enforcement agencies and with the support of Microsoft.

Internet piracy is an area in which we have much more to do to build anti-piracy capacity, but pro-active police and customs programs for fighting internet counterfeiting piracy, better technology tools used more widely, and better cooperation between the private sector and public authorities, must be the way forward.

[11] IFPI, Digital Music Report, at 21 (2005).

Conclusion

The goal of all anti-counterfeiting and anti-piracy activity is, of course, to protect the jobs, investment, economic activity, innovation and creativity that intellectual-property protections foster. In the internet age, anti-counterfeiting and anti-piracy also help to deter those who also would engage in hacking and other breaches of the computer security on which so much of modern society depends, and to deter those that would supply other illegal content. Microsoft stands ready to work both with the whole range of affected industries and with public officials to improve the technology needed to fight high-tech intellectual-property crime, and the public-private cooperation needed actually to deter and prevent piracy.