

Promoting the implementation of effective strategies and good practices by governments and business

Patrick De Smedt, Chairman, Microsoft Europe, Middle East and Africa

Good morning and thank you for giving me the opportunity to present the perspective from the private sector on how counterfeiting and piracy impact our industry and customers.

I will focus my remarks on the scale of the problem in our sector, and how this affects developing economies as well as developed economies, and small and medium sized businesses as well as large companies. I will also share our perspective on the role of technology and partnerships to combat these problems.

But let me preface these elements by reflecting on the contribution of intellectual property to the broader social good, since it is theft of IP that drives counterfeiting and piracy, and since there is a trend in some parts of government to downplay the need for robust IP laws and enforcement.

Intellectual property has inspired, and continues to inspire, social and economic progress. It provides the foundation for rewarding innovation and for providing further investment in R&D.

It is no coincidence that the gradual adoption of stronger IP laws worldwide since 1970 has coincided with tremendous advances in technology and exceptional growth in the number of firms and employees in technology industries.

At the same time, our industry is in the forefront of an acceleration of innovation and globalisation. This truly is the Digital Decade – in which not only leisure and lifestyle is going digital – and global - but so is the world of work, science and research, education and many other activities.

All of this means that the infrastructure for the digital world has to be very robust, and it also means that IP is increasingly a major source of competitive advantage not only for developed countries but also for developing countries as they aim to attract foreign investment and to move up the value-chain to maintain growth and job creation in their economies.

At Microsoft, intellectual property is central to all aspects of what we do. We depend for our success on two things.

The first is our ability to generate innovative and useful technologies.

The second is our ability to commercialize these innovations by transforming them into products and services that fulfill a market need.

And continued innovation is the only way for our company to grow.

Our R&D budget of almost \$8 Bio is one of the largest of any company in the world. So without robust IP protection, we and other technology leaders will not be able to maintain these levels of R&D investments.

When assessing current software piracy operations it is clear that they increasingly involve sophisticated, international networks of criminal groups. National governments play a critical role in providing the resources, legal tools, and political will necessary to dismantle these criminal operations.

The following examples highlight the sophistication, profitability and geographic reach of these criminal piracy rings and the critical importance

of international cooperation between law enforcement agencies and the industry:

- In a first example of last year ... the lead defendant in a massive German counterfeiting sting was sentenced to more than 5 years in prison. The case involved more than 250 German police and more than 80 raids nationwide. Law enforcement seized expensive watches, luxury cars, computers, and almost \$16 million in counterfeit software. The operation was suspected of selling \$200 million in counterfeit software annually and laundering profits through an international network of accounts.

- In a second example ... we are working closely with US federal and state authorities to dismantle a Russian criminal group engaged in global software counterfeiting, fraudulent spamming, and money laundering. Federal authorities in Russia raided the operation in 2004, seizing more than 70,000 counterfeit Microsoft software disks. We estimate that the group's counterfeiting revenues (for Microsoft products alone) are between \$400,000 to \$800,000 monthly.

One of the most important tasks for all of us is to share the role of educating the media, other parts of government and consumers about the problem, the victims and the cost involved.

So let me share with you some of the data on these costs.

As a key segment of the ICT industry, commercial software is more than a \$175 billion industry worldwide that generates jobs for 2.3 million people around the world.

The Business Software Alliance found that \$31 billion of software worldwide was pirated or counterfeit. This is why we welcome the initiative of the

OECD to conduct an industry survey on piracy and counterfeiting, as presented just before by Dr Wolfgang Hubner.

Beyond these direct revenue losses, rampant piracy limits our ability to fund innovation, to generate new jobs and tax revenues, to invest in emerging markets and to support a host of technology-based programs aimed at improving global education and achieving digital inclusion.

Indeed the Millennium Development Goals recognize the importance of technology access and technology innovation as key enablers of development in fields such as healthcare and education.

IP-based incentives and rewards are even more critical to small and medium sized enterprises.

Large technology companies increasingly license the discoveries and inventions of small firms to develop further breakthrough technologies.

At the same time, small businesses are far more dependent than large firms on the income derived from technology licenses.

In my sector, software, the amount of pirated software installed on PCs worldwide is 35% last year, representing the revenue losses of \$31 billion that I mentioned before but the losses for SME's are a staggering proportion of their revenues.

To help prove this point, allow me to give you an example of how counterfeiting endangers the small software companies.

Hermann Chinery-Hesse is one of Africa's most important software developers. His company in Ghana called 'Soft' occupies an important niche in the developing world's IT market.

Rampant piracy has hampered Soft's efforts to commercialize "mass market" applications developed by the company, and has also forced Soft to tightly control releases of its programs.

Hermann's creativity and innovativeness, and the products he and his company are producing are not enough to protect the future of this young and important enterprise. Such a company needs protection from governments in countries where its creativity is stolen.

In emerging markets inadequate IP protection is often the most significant trade barrier that we face as an industry. It is also a barrier to greater value-creation in the countries with those inadequate systems. Consider China for example which in 1996 was the sixth largest market for PCs and the 26th largest market for software.

Today, China is the second largest market for PCs but still only the 25th largest market for software. This growing disparity between hardware and software sales is directly attributable to a 90-plus percent piracy rate that has barely wavered in the past decade, despite China's repeated promises to strengthen IP protection and enforcement.

Now let me turn to our counter-strategies as a company and this in partnership with the industry and governments.

For almost two decades, Microsoft has worked to promote the use of legal software through a combination of company-specific initiatives and joint industry efforts in cooperation with the Business Software Alliance and other groups.

The Industry is very committed to coordinated actions, and the most recent proof of this commitment is the creation in October this year of BASCAP "Business Action to Stop Counterfeiting and Piracy".

Convened by the International Chamber of Commerce, BASCAP brought together in London CEOs from around the world representing the food and drink, pharmaceutical, textile, home products, finance, television, software and music sectors. Microsoft was represented by Steve Ballmer, our CEO.

The BASCAP participants agreed an initial, 4-point action plan:

- To create counterfeiting and piracy indices ... identifying issues that deserve greater attention within national IP protection programs
- To develop a clearinghouse to share best practices and strategies
- To compile a compendium of case studies and statistics – the first global, cross-sector stock take of the counterfeiting and piracy problem
- To develop educational materials for policy makers and the public to explain why IP rights should be respected and enforced.

This cross-industry CEO commitment and plan of action is very important to raise the profile of the problem to the highest levels of government and media attention.

For our part, Microsoft pursues a multifaceted strategy to fight software piracy and counterfeiting. In particular, we aim to

- (1) educate and protect our customers from being defrauded,
- (2) enhance the secure delivery of digital contents, and
- (3) strengthen intellectual property rights and enforcement of these rights.

So first we aim to educate and protect our customers from being defrauded.

To this end, we utilize overt and covert authentication technologies to deter piracy and aid consumers and law enforcers in the detection of illegal products. Counterfeit software is typically marketed as genuine product to unsuspecting consumers. To replicate the appearance of legitimate software counterfeiters use sophisticated technology to create "look-alike" copies of Microsoft CD-ROMs, packaging, documentation and other components. In more developed markets, counterfeit packages often include a combination of fake and genuine components.

To begin with the physical authentication features help consumers and law enforcement agencies in distinguishing legitimate software from sophisticated counterfeits, much in the same way governments authenticate their paper currency.

For example, our packaging includes a Certificate of Authenticity ("COA") that incorporates special inks, holograms and micro-text.

More recently, we developed a state-of-the-art hologram that covers the entire surface of the CD-ROM. Because these physical anti-counterfeiting features are increasingly difficult to replicate counterfeiters are now combining pirate CD-ROMs and packaging with genuine components, typically obtained through theft.

But physical authentication features are not enough.

It is estimated that today some 100 million households have gained broadband access. By the end of 2008, close to 200 million households will have broadband connections. Therefore online activation and authentication of products is critical.

We are giving our customers an incentive to buy legitimate products.

We provide additional value or services which are available for download ... only for legitimate users of Windows. When the consumer wants to get

these new features, they have to go through an authentication process which protects their anonymity.

If the consumer has installed counterfeit software in good faith they have the possibility to send their counterfeit product to Microsoft, and we will send them back a legitimate copy.

A second area of action is the distribution of digital content.

Recent figures from the International Federation of Phonographic Industries showed that the number of legal music tracks downloaded internationally tripled to 180 million in the first half of this year, while the volume of tracks being traded illegally rose only 3 percent to 900 million, despite the increased penetration of high-speed broadband lines.

Digital Rights Management (DRM) systems play a significant role in combating digital content piracy and counterfeiting.

According to a study from research firm Digital Tech Consulting some 311 Mio mobile hardware units capable of receiving such DRM-protected content as video and music will be shipped in 2009 up from 17 Mio last year.

Even more importantly, these technologies facilitate a variety of new online business models that promote electronic commerce and provide consumers with greater access to digitally distributed content.

DRMs make it easier for content owners to identify authors and articulate terms of use, to establish prices and collect payment, and to determine, among other things, how content is delivered, accessed and copied.

In recent years the IT industry has made tremendous progress in expanding the variety and improving the quality of DRM technologies.

To encourage broader use of DRMs and combat theft of digital content the Business Software Alliance and other IT industry groups are working to achieve legal remedies against circumvention of technical protection measures (TPMs) in accordance with the WIPO Copyright Treaties.

The TPM protections found in the European Software and Copyright Directives and the U.S. Copyright Act have helped to drive the rapid growth in online purchases of legitimate content.

A third area of action is Strengthening IP laws and enforcement

This is a multi-faceted strategy involving close partnership with government and industry. Microsoft works closely with legislators and government authorities to ensure that IP laws, enforcement activity and penalties keep pace with the growing threat of criminal counterfeiting and online piracy. We currently employ a worldwide anti-piracy and Internet safety team of 65 lawyers, forensic experts and investigators who partner with law enforcement agencies around the world.

Let me briefly mention 3 key areas of specific action:

- The first action is to achieve reform of domestic laws and international IP standards to strengthen protection and enforcement of intellectual property rights throughout the world.

In Europe the public and private sectors have long recognized the need for a Community patent to reduce administrative complexity and to streamline and harmonize the patent process.

This is especially true for small and medium enterprises which are not necessarily in a position to file applications in a number of EU countries at the same time.

- The second action is to reduce piracy and counterfeiting activity through civil, administrative and criminal enforcement actions.

In the US an example of that is that the Congress enacted in 2004 the "Anti-Counterfeiting Amendments Act of 2003" that prohibits brokering in genuine Certificates of Authenticity and other physical authentication components.

In Europe the Directive on the Enforcement of Intellectual Property rights adopted in 2004 is the centerpiece of the EU's ant piracy strategy. Among other measures, the Directive includes rules on searches and seizures provides for injunctive relief and harmonizes criteria for calculating damages.

Intellectual property rights are meaningless unless they can be enforced in practice. For this reason, we welcomed the EU Enforcement Directive.

- As third action area I want to highlight the use of technology to enhance collaboration between enforcement agencies.

Let me give you a practical example.

Microsoft has invested more than 4 million dollars in CETS the Child Exploitation Tracking System. CETS is a database housed within the National Child Exploitation Coordination Centre in Canada.

This database serves as an information repository and an investigative tool in law enforcement's fight against the online sexual exploitation of children. Officially launched in Canada in April this year, this system has already been used to prevent terrible crimes and to catch perpetrators.

Discussions are going on at the moment between our company and

various law enforcement agencies to roll-out CETS in other countries.

While this program is specifically about child exploitation, we appreciate that its features could serve other types of investigations.

Both we and law enforcement are going to learn a lot about the value of such a technology to fight criminality.

In conclusion, I would like to emphasize the need for even more partnerships between industry and law enforcement.

Given the complexity and scale of the counterfeiting and piracy challenge and the crucial role of law enforcement agencies in tackling it we are committed to a partnership approach.

We believe that more such partnerships are needed as part of the coordinated and collaborative response by society. We know there is more to be done that more resources are needed but we already see some innovative partnerships we may learn from as they demonstrate new ways of exchanging information and intelligence.

For instance in the US the Digital PhishNet is a joint enforcement initiative between industry and law enforcement designed to ensnare those who perpetrate phishing attacks. That is unsolicited communications which aim to defraud the recipients.

The goals of PhishNet are simple to identify, arrest and hold accountable, those that are involved in all levels of phishing attacks.

Currently members include Internet service providers online auctions financial institutions which work with law enforcement to include the FBI, Secret Service, US Postal Inspection Service and the Federal Trade Commission.

In Europe the European Commission is supporting the industry in launching a new project called Spotsam which aims at facilitating the establishment of a European network of antispam hotlines.

The ultimate purpose of Spotsam is to help enforcement authorities to get relevant complaints and facilitate their work hence permitting the creation of an ecosystem where the private and public sector work together to make the Internet safer.

Microsoft is involved in these two projects, and will be keen to share the lessons we will learn from these and from the other initiatives I have described today to pursue our common goal to reduce counterfeit for the benefit of consumers and local economies.