Addressing Global Software Piracy

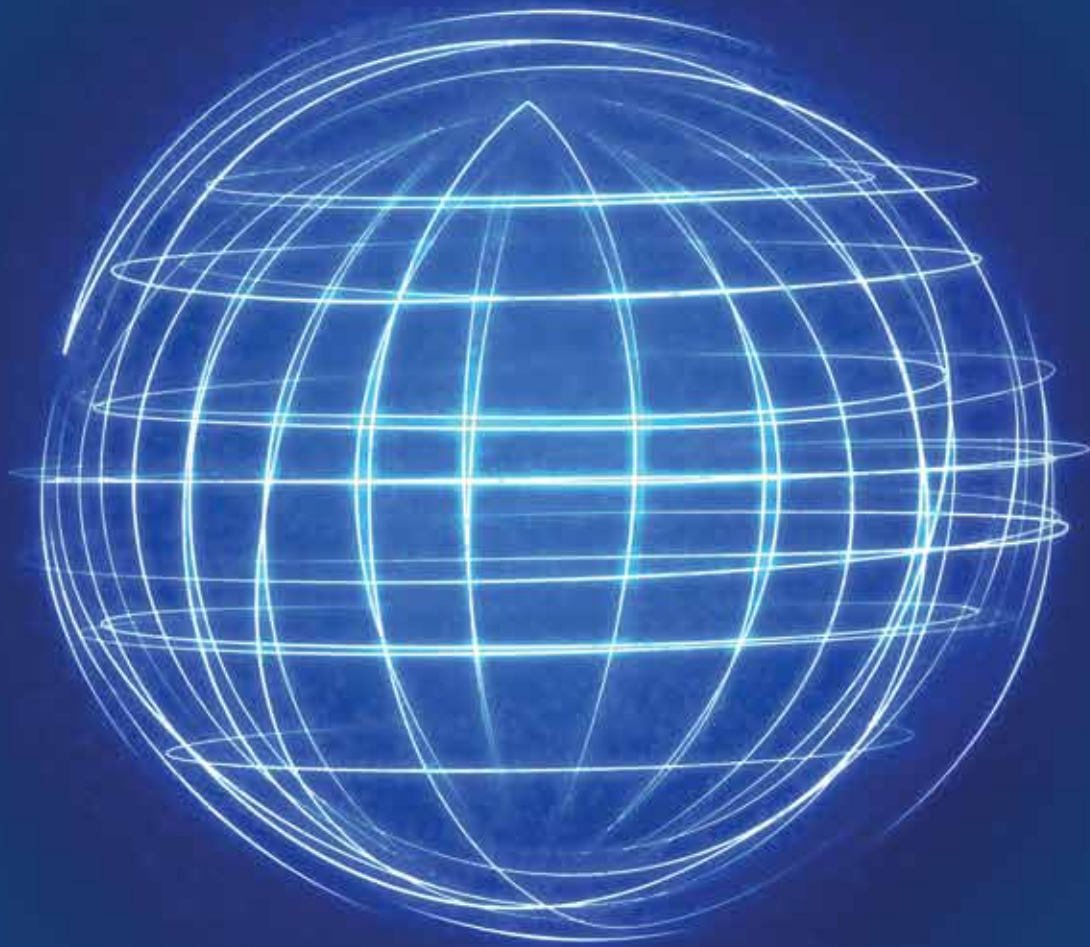Partnering with Governments, Industry, and Customers to Strengthen Economies, Drive Innovation, and Protect Information Systems

Addressing Global Software Piracy

Partnering with Governments, Industry, and Customers to Strengthen Economies, Drive Innovation, and Protect Information Systems

The global information technology (IT) industry is a vital driver of economic growth, employing more than 35 million people worldwide and generating an estimated US$3 trillion in spending around the globe. This vibrant IT "ecosystem" exists in large part due to an ongoing cycle of investment and innovation by hundreds of thousands of software, hardware, and IT companies—many of them small and locally owned. These companies rely on intellectual property (IP) systems that offer protections and incentives to develop new ideas, bring them to market, and share them with other innovators.

Ensuring the health of the IT ecosystem and the IP incentives that drive investment and innovation is important in the current economic climate for both established and emerging markets. A healthy and legal technology sector has long been a significant factor in the growth and vitality of established economies. Likewise, emerging markets are increasingly recognizing the importance of IP as they invest in becoming knowledge-based economies.
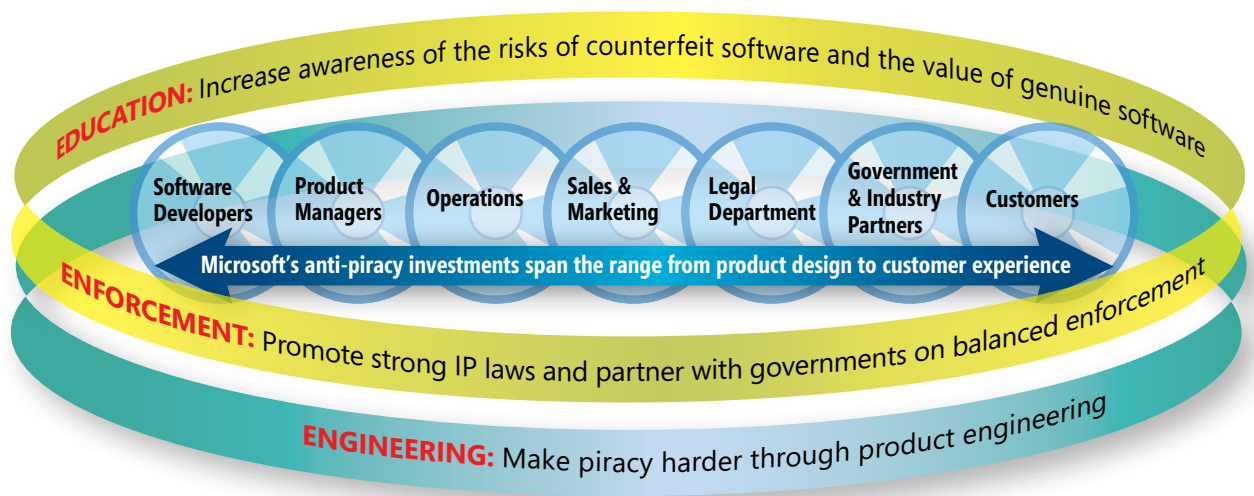
The loss of economic value through IP theft, including counterfeiting and piracy, results in millions of lost jobs, an estimated US$750 billion in lost global revenues annually, and health and safety risks from unsafe products. International criminal syndicates counterfeit and pirate

Policy Briefs from Microsoft

A convergence of innovative software and intelligent devices, complemented by cloud-based services, will stimulate economic growth, make government more effective, and benefit citizens in areas ranging from education to healthcare to the environment. This policy brief is one in a series from Microsoft about next-generation computing.

Microsoft's Comprehensive Approach to Addressing Software Piracy

EDUCATION: Increase awareness of the risks of counterfeit software and the value of genuine software

Software Developers · **Product Managers** · **Operations** · **Sales & Marketing** · **Legal Department** · **Government & Industry Partners** · **Customers**

Microsoft's anti-piracy investments span the range from product design to customer experience

ENFORCEMENT: Promote strong IP laws and partner with governments on balanced enforcement

ENGINEERING: Make piracy harder through product engineering

the IP of a diverse array of industries and companies, including Microsoft and our partners. These criminal rings have developed international counterfeiting production and distribution networks, digital piracy infrastructures that touch virtually every corner of the globe, and sophisticated fraud schemes to gain access to products and services offered by Microsoft and our partners. Increasingly, software pirates are involved in other types of criminal behavior, including online fraud and identity theft, child exploitation, money laundering, narcotics trafficking, and violent crime.

Microsoft is the world's largest software company, with nearly 90,000 employees in over 100 countries; our products and services are supported by over a half million IT partners worldwide, from large multinational computer manufacturers to small local system builders and software service providers and developers. Nearly 15 million people are employed by Microsoft partners in every part of the globe, generating revenues that remain in local communities to drive economic growth and new social opportunities.

To address the threat posed by global software pirates, Microsoft has built a worldwide anti-piracy team that tracks and traces criminals in more than 150 countries and works closely with law enforcement to support criminal prosecutions. This team includes former police officers and prosecutors, IP attorneys and specialists, intelligence analysts, forensics experts, and government affairs professionals.

In collaboration with other companies and with industry associations, Microsoft works with legislators and policymakers on the enactment and implementation of laws and policies that protect IP incentive systems and allow them to thrive. We also work closely with customers who inadvertently receive counterfeit or pirated software, to provide them with genuine software and to identify the counterfeit suppliers. In the past two years, the number of leads and reports we have received from customers about vendors suspected of selling counterfeit software has more than doubled to over 150,000. This dramatic increase in customer engagement in identifying the sources of counterfeit software reflects our customers' increasing concern about the threats posed by such counterfeits. The critically important partnerships between Microsoft, industry members, governments, partners, and customers are the cornerstone of our approach to addressing piracy.

COUNTERFEIT

COUNTERFEIT

GENUINE (LEFT), COUNTERFEIT (RIGHT)

GENUINE (LEFT), COUNTERFEIT (RIGHT)

High-quality counterfeits are intended to deceive customers, and they pose significant security and functionality risks.

The Risks of Counterfeit Software

The security risks to individuals, businesses, and governments posed by counterfeit and pirated software are significant and increasing. One seminal study by the market intelligence firm IDC in 2006 found that one in four Web sites offering counterfeit software attempted to install unwanted or malicious code upon downloading.[1] The study also described a review of counterfeit Microsoft software purchased at resellers in 17 countries, which determined that more than 50 percent contained phony code or malware or could not even be installed. A 2009 study by the Business Software Alliance and IDC concluded that countries with high piracy rates often have high malware infection rates.[2]

A recent Microsoft study highlighted these dangers and how easy it can be for customers to unknowingly install risky software.[3] A review of 30 mid-size businesses in the United Kingdom found that more than one-third of the companies were unknowingly using counterfeit software. These businesses spent an average of US$10,000 on the software. Each company reported purchasing the software in good faith and expressed shock that it was not genuine.

The impact of using counterfeit software can be serious and costly. The effects of malware can range from annoying advertisements to a severe breach of information security. A recent Harrison Group study found that companies using pirated or counterfeit software were 73 percent more likely to experience loss of or damage to sensitive data and 43 percent more likely to have critical computer failures lasting 24 hours or longer.[4] Recovery from an incident of malicious software on a single workstation can exceed US$1,000, and the costs due to lost or compromised data can run into the tens of thousands of dollars per incident. Individuals and organizations that knowingly purchase pirated or counterfeit software in the hopes of saving money can see those savings—and much more—wiped out with a single security breach.

---

[1] "The Risks of Obtaining and Using Pirated Software," IDC white paper, sponsored by Microsoft (October 2006).

[2] "Sixth Annual BSA-IDC Global Software Piracy Study," Business Software Alliance and IDC (May 2009).

[3] "The Surprising Risks of Counterfeit Software in Business," Microsoft white paper (2009).

[4] "Impact of Unlicensed Software on Mid-Market Companies," Harrison Group (September 2008).

Software Piracy Rate

Worldwide, 41% of software in use is pirated.

41% pirated software

59% genuine software
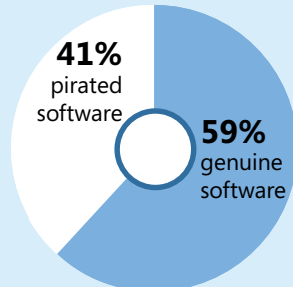
Source: "The Impact of Software Piracy and License Misuse on the Channel," IDC, June 2008.

Piracy Reduction Impact

Global economic benefits from a 10 percent reduction in software piracy:

+**$141 billion*** contribution to GDP

+**$24 billion*** additional tax revenues

* in US dollars

+**600,000** new jobs

Source: "The Economic Benefits of Lowering PC Software Piracy," IDC, January 2008.

For every dollar that Microsoft realizes from reduced software piracy...

$1 = **$5.50**   INCREASED REVENUES   LOWER COSTS

...other companies in the software ecosystem will realize $5.50.

The Economic Benefits of Increasing Legal Software

Alarmingly, software piracy is on the rise. The global software piracy rate increased 3 percent between 2007 and 2008, to 41 percent.[5] This increase was driven primarily by double-digit growth in the market for personal computers in developing countries and regions with high software piracy rates. However, even in countries and regions with lower piracy rates—such as the United States, Japan, and Western Europe—pirated software can be found on one in every five PCs. Even more alarming is the increase in global economic losses from software piracy, which amounts to a staggering US$53 billion annually.[6]

The good news is that even an incremental reduction in software piracy can have dramatic benefits for the global economy. Lowering the piracy rate by just 10 percent would create an estimated 600,000 new jobs worldwide and contribute US$24 billion in additional tax revenues to local and national governments.[7] In addition to supporting governments and their local and national economies, these economic benefits would flow to hundreds of thousands of legitimate businesses. For every dollar that Microsoft realizes from lower software piracy, other companies in the software ecosystem will realize a total of $5.50 from increased revenues and lower costs.[8]

[5] "Sixth Annual BSA-IDC Global Software Piracy Study," Business Software Alliance and IDC (May 2009).

[6] Ibid.

[7] "The Economic Benefits of Lowering PC Software Piracy," independent study by IDC, sponsored by the Business Software Alliance (January 2008).

[8] "The Impact of Software Piracy and License Misuse on the Channel," IDC white paper, sponsored by Microsoft and the International Association of Microsoft Certified Partners (June 2008).

# Public-Private Collaboration: The Key to Combating Piracy

The growing global threat of software piracy is one that neither governments nor the IT industry can tackle alone. Government and industry cooperation on a range of enforcement and policy issues is crucial to ensuring that officials have the tools they need to address piracy effectively. Microsoft and our local partners are working with governments, other industry members, and trade associations to provide training and other needed collaboration on anti-piracy issues.

When industry-government partnerships on IP incentives are strong and sustained, the benefits that flow to economies and society are significant. One powerful example is the partnership between the software industry and the Russian government. In 2007, Russian authorities and the software industry began collaborating on an IP awareness and enforcement campaign. This campaign was designed as a sustained effort to support legal software innovation, distribution, and use. It included training for hundreds of law enforcement officials in investigating and prosecuting software pirates and led to more than 3,000 criminal raids in a single year.

The effort also included a highly visible public awareness campaign in multiple Russian cities about the risks of piracy. The results were dramatic. Software piracy in Russia dropped a record 7 percent in 2007, and another 5 percent in 2008. These gains have contributed millions of dollars and thousands of jobs to local IT companies (including Microsoft partners) and the Russian economy and have led to an environment in which legal software innovation can flourish in the future.

Year-Over-Year Software Piracy Rates in Russia

80%
73%
68%

2006   2007   2008
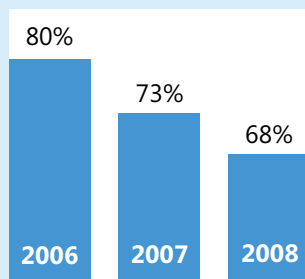
Collaboration between the Russian government and the software industry has resulted in steady declines in business software piracy.

Government tax audits of businesses have resulted in the collection of millions of dollars in tax revenues from the use of pirated software and dramatic declines in software piracy rates.

Another example is the campaigns in Colombia, Serbia, Italy, and Greece that require software inspections during tax audits of businesses. This approach, which also includes the enactment of relevant IP and fiscal laws, training, and cooperation with the private sector, has led to measurable drops in overall software piracy rates and increased tax revenues in all four countries.

In Colombia, the tax inspection law requires companies to include in their annual reports a declaration of compliance with copyright laws, and it empowers the Colombian Tax and Customs Administration (DIAN) to inspect software licenses during routine tax inspections. The law treats software piracy as a form of tax evasion. According to DIAN, Colombia's value-added tax revenue from the software industry grew $87 million between 2008 and 2009.

In Serbia, tax inspectors audited more than 1,000 companies in 2008 and filed more than 100 complaints with the public prosecutor's office for alleged use of pirated software. The Serbian software piracy rate has begun to decline and is expected to decline even further due to the government's efforts in this area. In Italy, the program led to a dramatic decline in software piracy rates, from 92 percent in 1991 to 55 percent in 1996. In Greece, the software piracy rate decreased by 7 percent from 2005 to 2008. Based on these positive outcomes, we recommend that every country, particularly those in emerging markets, seriously consider adopting a tax audit initiative that supports the use of legal software.

Dismantling Criminal Syndicates

Strong enforcement against criminal syndicates is another critical building block in an effective global anti-piracy strategy. In the largest counterfeiting case in history, Microsoft worked with law enforcement authorities in China and the U.S. to build a high-profile case against a criminal syndicate based in southern China. This software counterfeiting ring is believed to be responsible for producing US$2 billion in counterfeit Microsoft software between 2003 and 2008 and distributing it to unsuspecting customers in at least 36 countries.

The China Case

- Evidence gathered from over 1,000 customers and partners

- 19 different products in 11 languages found in 36 countries

- $2 billion+ in counterfeits produced

- 11 members of the counterfeiting ring, including the ringleaders, convicted and sent to prison

On December 31, 2008, the Futian People's Court in Shenzhen, China, convicted 11 members of the counterfeiting syndicate and sentenced them to prison terms ranging from 1½ to 6½ years—the longest sentences ever handed down in China for IP rights violations. This landmark case was the result of unprecedented international cooperation between U.S. and Chinese law enforcement officials, who, together with Microsoft and our local partners, developed leads and evidence from more than 1,000 Microsoft customers and partners victimized by the syndicate.

While this case was a major breakthrough, much more remains to be done in China and other countries to limit the volume of counterfeit software being produced and distributed, and to protect consumers from the risks of using fake software.

Microsoft forensics experts use intelligence to trace counterfeit discs to their source.

Supporting Governments with Intelligence, Innovation, and Expertise

Our collaboration with international, national, state, and local law enforcement on software piracy investigations has resulted in raids, seizures, and arrests of IP criminals in virtually every country in the world, including many smaller emerging economies that increasingly understand the importance of a healthy, legal technology sector. Microsoft is committed to maintaining and expanding cooperative anti-piracy efforts with governments across the globe to ensure that police, prosecutors, border authorities, and the judiciary have the tools and assistance they need to address counterfeiting and piracy more effectively.

Microsoft has developed a variety of forensic and intelligence systems to support our anti-piracy efforts. Nine regional forensic crime labs around the world examine and process suspected counterfeit software. In 2008, these labs evaluated more than 500,000 pieces of evidence that were used to support both civil and criminal cases and for business intelligence. A significant amount of this evidence came directly from our customers and partners through tips and voluntary product submissions.

Microsoft has also invested in technologies that enable us to "connect the dots" between pieces of evidence. These technologies identify "fingerprints"—specific physical characteristics—of counterfeit discs and match them to fingerprints of other known counterfeit software. This enables Microsoft and law enforcement officials to trace illegal discs to the criminal syndicates that produced them and to estimate production volumes. For example, in the China case, we linked thousands of counterfeit discs—encompassing 19 different Microsoft products in 11 languages—to the same syndicate. We've also developed improved techniques to detect malicious code and spyware in counterfeits sold to unsuspecting consumers around the world.

One of the latest breakthroughs in anti-piracy forensics is a tool that works remotely to determine the manufacturing facility where counterfeit discs were produced. The tool "reads" data error patterns unique to each Laser Beam Recorder (LBR) used in mastering. These unique LBR fingerprints are matched to fingerprints in our extensive library of discs from known counterfeit manufacturing facilities. When a disc exhibits the same characteristics, we can trace the counterfeit to a particular facility.

Left: Disk-specific "fingerprints" help Microsoft forensics experts and law enforcement uncover criminal counterfeiting syndicates. Right: Microsoft interactive holograms help customers detect counterfeits.

Microsoft also relies heavily on business intelligence in our anti-piracy efforts. Our global anti-piracy team routinely monitors the marketplace through data mining, mystery shopping, test purchases, and other internal and public intelligence sources to identify pirate suppliers and piracy trends. This intelligence enables us to uncover the sources of piracy and address them with technology solutions and enforcement. It also helps us better protect our customers and partners from the risk of counterfeits and follow up on the tips they provide.

Microsoft's arsenal of forensic tools and capabilities enables police and prosecutors to get the full story behind a single test purchase or seizure of evidence. The intelligence ties counterfeit software to particular production facilities and to known counterfeiting syndicates, and it demonstrates to judges and juries the true extent and nature of the damage that has been caused. We will continue to invest in innovative technologies and anti-piracy forensics that allow us to partner effectively with governments in responding to this increasingly complex global threat.

Building Stronger Partnerships for the Future

The wide range of software, services, and computer and communication devices available today enables people and businesses to pursue their ideas and opportunities in ways only dreamed about a decade ago. A decade from now, the possibilities created by technology innovations will be equally groundbreaking. As Microsoft's vision of "life without walls" becomes a reality for the billions of people connected through personal computers, mobile devices, and the Web, protecting the integrity of the world's technology infrastructure, and the intellectual property that fuels it, will become increasingly critical.

To fully realize the benefits from innovation and a system of IP incentives, our partnerships and collaborations must grow and strengthen to meet new challenges. We will need continued improvements in our investigative and analytical tools and skills, more robust and effective international cooperation and coordination in investigations and prosecutions, more effective IP laws and enforcement rules, and increased commitments by governments around the world to programs that protect IP. Only then will we be able to succeed against the multi-billion-dollar global threat of counterfeiting and piracy and fully realize the economic growth and social opportunities that a healthy, legitimate technology ecosystem can help create.

For the online version of this document and more information about our Public Policy Agenda, please visit www.microsoft.com/publicpolicy.

Microsoft