Online Piracy Global Perspective and Trends
Panama, April 2012

Mo Ali
Head of Internet Anti-piracy Operations
mo@ifpi.org
• IFPI (International Federation of the Phonographic Industry) represents the recording industry worldwide with some 1400 members in 66 countries and affiliated industry associations in 45 countries including Ukraine

• IFPI's international Secretariat is based in London and is linked to regional offices in Brussels, Hong Kong and Miami

• IFPI's mission:
  – Promote the value of recorded music
  – Safeguard the rights of record producers
  – Expand the commercial uses of recorded music
Overview

• Outline of the problem

• Current and future threats

• The industry’s response
The Challenge

95% of music downloads worldwide unlicensed and illegal; no revenue to artists or producers

- 55% P2P
- 45% Non-P2P
% of unlicensed users that access P2P and non-P2P services

<table>
<thead>
<tr>
<th>Country</th>
<th>P2P</th>
<th>Non-P2P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mexico</td>
<td>55%</td>
<td>45%</td>
</tr>
<tr>
<td>Argentina</td>
<td>51%</td>
<td>49%</td>
</tr>
<tr>
<td>Chile</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>Brazil</td>
<td>32%</td>
<td>68%</td>
</tr>
<tr>
<td>Latin America</td>
<td>46%</td>
<td>54%</td>
</tr>
</tbody>
</table>
From the outside looking in

% on internet users accessing at least one unlicensed service (Feb 2012)

- Argentina: 79%
- Chile: 73%
- Mexico: 68%
- Spain: 44%
- Brazil: 43%
- France: 24%
- Global: 28%

Source: Nielsen and comscore
From the outside looking in

% of unlicensed users accessing BitTorrent and non-BitTorrent P2P services

<table>
<thead>
<tr>
<th>Region</th>
<th>Non-BitTorrent</th>
<th>BitTorrent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mexico</td>
<td>87%</td>
<td>13%</td>
</tr>
<tr>
<td>Argentina</td>
<td>84%</td>
<td>16%</td>
</tr>
<tr>
<td>Chile</td>
<td>73%</td>
<td>27%</td>
</tr>
<tr>
<td>Brazil</td>
<td>40%</td>
<td>60%</td>
</tr>
<tr>
<td>Latin America</td>
<td>73%</td>
<td>27%</td>
</tr>
</tbody>
</table>

Source: Nielsen and comScore
The Challenge

DIGITAL  PHYSICAL

LITIGATION  LOBBYING
The threat, the challenge

• Peer to Peer (P2P)
  – Content held on end users’ computers
  – Core Protocols:
    • BitTorrent
    • Gnutella
    • DirectConnect
    • eDonkey
    • Ares
  – Web sites, centralised hubs and trackers are core / fundamental parts of file distribution architecture

• Non Peer to Peer
  – Content held on central server resources
  – Structured infrastructures
  – Move to “The Cloud”
  – Move towards the “Business Criminal”
The threat, the challenge

• Non Peer to Peer (P2P)
  – Hacking / Phishing
  – Release Groups / Top Sites / Pre-release
  – Blogs / Forums / Cyberlockers / Link Aggregators
  – Direct Download Sites and Deep Lining Sites
  – Social Networking Sites
  – Streaming and UGC Sites
  – Newsgroups / USENET
  – Mobile Data Networks
  – Proxies / Commercial Virtual Private Networks
Hacking / Phishing

• Email accounts of management and artists targeted
• Bogus emails sent pretending to be from email/cyberlocker/social networking provider
• Using the password reset function to access account – most common security questions, place of birth or mother’s maiden name
• Once compromised account monitored, locked out or emails forwarded to another account
• Trojan files can lead to RAT (remote access tool) software being installed – PC only
Mobile

- Illegal downloading and sharing of content across the mobile data network but also across wireless roaming.

- Current generation mobile devices have similar Internet functionality as PCs; net based integration increases productivity.

- Standard browsers facilitate download and streaming from ‘traditional’ sources.

- Many ‘specialist’ PC applications ported to mobile environment; Apple and Android architectures in particular encourage 3rd party development.
Mobile

- Gartner: By 2025 the number of mobile connections worldwide will reach 50 billion
- Gartner: 100% per year growth on mobile devices
- Morgan Stanley: By 2015 more people will connect to the Internet via mobile devices than via desktop PCs
- All you can download monthly plans fuelling problem although TelCos starting to see bandwidth saturation
- ‘Challenges’ in matching IP address to subscriber
Potential Connection Speed (Mbps)

<table>
<thead>
<tr>
<th>Technology</th>
<th>Potential Speed (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5G (GPRS)</td>
<td>0.056</td>
</tr>
<tr>
<td>2.75G (EDGE)</td>
<td>0.2368</td>
</tr>
<tr>
<td>3G</td>
<td>5.8</td>
</tr>
<tr>
<td>4G</td>
<td>100</td>
</tr>
</tbody>
</table>

General Packet Radio Signal / Enhanced Data rates for GSM Evolution
Mobile

% of Mobile Data

- **P2P**
- **HTTP Streaming**
- **HTTP Browsing**
- **HTTP Download**
- **Other App**

Global vs EMEA

Stats from [http://www.internetworldstas.com](http://www.internetworldstas.com) and Allot Communications.
Mobile

• Crawling of Apple App Store and Google MarketPlace

• Focus on quick take down agreements with app stores; Apple, Google, Microsoft, Nokia (IFPI Finland) and Palm

• Close liaison between RIAA, IFPI and National Groups

• Possible expansion of payment provider programme to target ‘rogue’ – typically Android – app developers

• Given browser focus of user activity, ensure content source impacted via notice and takedown programme
Cloud

- Wikipedia: Cloud computing describes computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services;

- Provides cheap, dynamic and expandable computing power

- New level of service providers i.e. cloud providers added to the equation with regards to securing evidence, potential litigation and notice and take down

- More commonly the term Cloud is used to described centrally located, Internet based resource i.e. Processing, storage, redundancy
236 lockers were tracked in 2011, the top 10 lockers accounted for 75% of infringing URLs found.

Stats source: IFPI’s Internet Anti-Piracy System
Cloud

• High volume notice and take down; automated reporting and takedown

• Online services that distribute or facilitate access to content:
  – preferably, proactively filter for infringing content
  – if not, operate an effective and efficient notice and take down system
  – Otherwise; shut down

• Licensing v Anti-Piracy
The Business Criminal

• Designs a business model around piracy

• Designs, hosts and structures in such away to maximise ‘up’ time; this includes manipulation/anonymization of Domain Name Service and Whois records and exploitation of weak laws and/or legal loopholes

• Maximise revenue with secondary hosting and advertising deals in addition to any direct i.e. paid for downloads or contributions revenue
The Business Criminal

• It used to be about the kudos of being the first to obtain and leak content

• Growing trend around ‘leaking for profit’; either monetary or reputation

• As release protection procedures have been improved and content reviewed digitally the source i.e. Artists, labels, management, producers is being targeted

• Risk for targets goes beyond loss of un-released content
Russian / Ukrainian download sites

• Websites distributing unlicensed sound recordings via download for payment

• 50 + such sites identified

• Music albums sold for as little as Euro 0.64 cents

• Have the appearance/interface of being legal

• Allofmp3 – at its height – second only in popularity to iTunes

• UK/US facing, in English and tailored to the UK/US market
In Excess of 50 Russian/Ukrainian Download Sites
Album Price
Euro 0.64
Russian / Ukrainian download sites

A partnership approach has been fundamental to our success to date

(Economic Crime Unit)

IFPI Members

The Law
The wider benefits that the program provides

- Law enforcement have secured evidence that the illegal sites are annually stealing hundreds of millions of dollars hence the program is therefore of the upmost importance to the global recording industry.
- Creating opportunities for further linked LE investigations such as money laundering and tax evasion.
- It removes a revenue stream from organised crime which would undoubtedly be reinvesting the funds into other serious crime.
- It creates skill exchange opportunities between the public and private sector.
Next steps

• Engage other payment providers
• Evaluate criminal profit / loss to industry
• Recover proceeds of crime
• Together with the City of London Police engage with Interpol to scope out the next international steps:
  • Launch the initiative in other countries
  • International asset confiscation coordination
  • Engaging with the international financial services sector to secure their cooperation in the partnership approach
Advertising

• Disruption of revenue streams

• Structured notice and take down programme targeting Google’s AdSense and DoubleClick advertising networks

• Out reach to IASH and IAB to implement comprehensive infringing block list

• Direct contact with advertisers flagging issue of illegal / infringing site usage
The threat, the challenge
The threat, the challenge
The challenge

• Thousands of potential distribution points, the majority of which need some form of monitoring; significant risk of information ‘overload’

• Different protocol/channel, different technology; rapidly changing operational environment

• The best approach?
  – Take down
  – Disruption
  – Investigation
  – Lobbying
  – Litigation
The response

• Dedicated Anti-Piracy staff
  – Primary focus on online but core physical skills retained
  – Central London operation with National Group coverage in 35 countries
  – 24/7 coverage
  – Structured covert investigations resource
  – Law Enforcement liaison and training programme

• Co-ordination of global pre-release and high volume site/content take down programme
  – Direct company liaison
  – Leak notification
  – Comprehensive reporting

• Automated system / application development

• Litigation & lobbying support
The response

• Over 15 million infringing URLs removed in 2011
  – Structured and highly automated notice and takedown programme
  – Targeted programme to impact site operation and reputation
  – Visibly disrupt the supply chain and visibility of infringing content

• Strategic litigation / Strategic action
  – The PirateBay
  – Demonoid
  – LimeWire

• Payment / Ad providers
  – Agreements with VISA, MasterCard, PayPal, CTIA, Monitise, PaySafeCard and PhonePayPlus
  – Expanding scope to other providers and beyond www
  – Strategic agreements with other industry partners
The response

• Online services that distribute or facilitate access to content:
  – Preferably, proactively filter for infringing content
  – If not, operate an effective and efficient notice and take down system
  – Otherwise, shut down

• Internet Service Providers:
  – Should not provide internet access to infringing sites / services or unidentified customers
  – Block access to infringing sites / services located outside the local jurisdiction
  – Implement a system of graduated response for infringing P2P users including warnings to an effective deterrent sanction
End User Evidence - Overview

- Evidence provider has its own P2P client software, which essentially works the same way as the regular clients.

- The software connects to other P2P users and communicates with them using a standard file-sharing protocol i.e. works / interacts just like a human would.

- Evidence provider simply automates the process of collecting information which is publicly available on the file-sharing networks.

- Content verified by 3rd party fingerprint process.
**P2P Overview**

### Identify
- Use keywords to locate and identify content

### Verify
- Verify Asset:
  - Manual
  - Automated
  - Asset Verified?
    - Yes
    - Generate Verified Hashes
    - No

### Act
- Generate Information:
  - Asset being infringed
  - Verification mechanism
  - Asset has Verified Hash?
    - Yes
    - Generate Verified Hashes
    - No

### Infringer
- Identify IP addresses that are sharing that content

- Verify IP address
  - IP address Verified?
    - Yes
    - Generate Information:
      - Infringing IP address
      - Verification mechanism
    - No
      - Discard

- Take Action
End User Evidence

• Court standard evidence provided for each case

• Full verification available given start to end packet trace process

• Automated process mirrors end use experience and process

• Summary provided to ISP, full evidence packs available via secure download
Blocking - Overview

- A variety of technical measures can be used by an ISP seeking to block access to websites. All of these methods use the kind of network technologies that are typically already in place at a large ISP and in some form of configuration for the purpose of network protection, network management and/or security.

- The main technical options for consideration as mechanisms to allow blocking are the use of access control lists (ACLs)/IP address, domain name service (DNS), deep packet inspection (DPI) and/or proxies.

- The effectiveness of such a “block” will depend on the determination of the ISP subscriber and the content/website provider to maintain access to each other and to use circumvention techniques to bypass blocking techniques. There is evidence to suggest that there is limited (between 3% and 5%) adoption of these circumvention techniques although subscribers with more technical knowledge could look to circumvent ISP controls using virtual private networks (VPN) or anonymous proxies.

- Combinations of blocking methods have been proven to work in a commercial environment i.e. British Telecom’s CleanFeed and recent court approved site blocking orders.
Technical Options – DNS

UNSUCCESSFUL DNS RESOLUTION
DNS RESPONSE SAYS NOT FOUND

WEB REQUEST NOT MADE
BROWSER RETURNS
SITE NOT FOUND, or such
Technical Options – IP / Router

- DSLAM (ISP)
- Aggregation & Backhaul
- ISP Access Control
  - Proxy
  - DPI
  - RADIUS
- Core Network
- Transit Network
- Internet
- Home PC
- CPE
-成功DNS解析
-路由器识别可疑IP &
  黑洞流量，或发送重置等
  浏览器超时，或
  服务器重置
Technical Options - DPI

DPI recognizes and bounces Web request.

Proxy double checks URL & serves, forbidden access message.

Successful DNS resolution.

ISP access control.
The PirateBay & BTJunkie Usage - Italy
# Blocking – Court Actions

<table>
<thead>
<tr>
<th>Implemented</th>
<th>Country</th>
<th>Blocking type</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2011</td>
<td>Austria</td>
<td>IP and DNS</td>
</tr>
<tr>
<td>September 2011</td>
<td>Belgium</td>
<td>IP and DNS</td>
</tr>
<tr>
<td>Oct 06/May 10/Feb 12</td>
<td>Denmark</td>
<td>Not specified/DNS/Not specified</td>
</tr>
<tr>
<td>January 2012</td>
<td>Finland</td>
<td>IP and DNS</td>
</tr>
<tr>
<td>February 2012</td>
<td>India</td>
<td>IP, DNS and URL DPI</td>
</tr>
<tr>
<td>July 2009</td>
<td>Ireland</td>
<td>IP and DNS</td>
</tr>
<tr>
<td>November 2011</td>
<td>Israel</td>
<td>Not specified</td>
</tr>
<tr>
<td>Dec 09/Jul 11</td>
<td>Italy</td>
<td>IP and DNS (for both cases)</td>
</tr>
<tr>
<td>January 2012</td>
<td>Netherlands</td>
<td>IP and DNS</td>
</tr>
<tr>
<td>October 2011</td>
<td>UK</td>
<td>IP and URL DPI</td>
</tr>
</tbody>
</table>
Blocking - Conclusion

• In the majority of cases the technical infrastructure required to facilitate website blocking already exists within major ISPs

• Rulings have show that Courts accept that site blocking has a fundamental role to play in the protection of copyright on the Internet

• Legislative momentum continuing to build with rulings pending/discussions in progress in Austria, Belgium, Germany and the Netherlands

• Effectively deployed ISP blocking methods have been proven to have a significant impact on the behaviour of the vast majority of website users who are typically neither technically aware or inclined to seek out circumventions

Strictly Privileged and Confidential
The response

• Working together - Law Enforcement
  – Facilitate knowledge exchange, liaison, training and relationship building
  – Ongoing case referral and intelligence management programme
  – Case generation / liaison is the best form of training

• Working together - Judges, Legal Bodies
  – Rapidly changing legal and operational environment
  – Opportunities to provide training built around ‘real world’ experiences and challenges rather than focusing on theory

• Working together - Partners
  – Education
  – Shared knowledge, shared resources
  – Help facilitate a greater impact on illegal activities
Summary

• Technical challenges will grow with online population; technical enforcement solutions must be developed to meet the challenge

• Skill sets across all areas of investigation, analysis and prosecution need to be maintained and developed accordingly

• Co-operation, partnerships and information exchange are fundamental to ongoing success

• Amendments to relevant laws need to plan for the future

• Consider ‘quick, curve ball’ solutions to impact more complex operations as complement to long term investigations
Summary

‘THE TEAM’
TECHNOLOGY
CONTENT PROTECTION
INTERMEDIARY
LITIGATION & LOBBYING
PARTNERS
PROSECUTORS LAW ENF
EDUCATION
Thank You

Mo Ali
Head of Internet Anti-piracy Operations
mo@ifpi.org