



## **BSA Recommendations to United Kingdom Government Regarding Implementation of the Enforcement Directive**

### **Executive Summary**

**The widespread and unchecked phenomenon of intellectual property rights infringement is causing creative industry in the United Kingdom severe financial loss, posing a threat to the viability of certain sectors of that industry. The United Kingdom Government has the opportunity to address this problem by enacting a robust implementation of the Enforcement Directive<sup>1</sup>, most notably in relation to (i) urgent and long-needed changes regarding damages awarded in intellectual property matters, and (ii) civil search and seizure order procedure.**

### **Introduction**

The Business Software Alliance (“BSA”) represents a broad cross-section of commercial software publishers, from multinational software providers to smaller, European suppliers such as UK based Monotype Imaging. These organisations rely on robust intellectual property enforcement frameworks to protect their rights. Deficiencies in these frameworks in the UK are stifling development and creativity by creating an environment in which abuse of intellectual property rights (“piracy”) is thriving.

BSA estimated that in 2004 (the most recent year for which figures are available), piracy resulted in losses of over £1 billion being suffered by the UK software industry<sup>2</sup>. Piracy losses at this level are unacceptable. The impact of these losses is not just confined to the software industry: an IDC economic impact research study, commissioned by BSA in 2003, estimated that achievable decreases in piracy would result in an additional £2.5 billion worth of tax revenues to the UK Government. Piracy is costing the UK taxpayer billions of pounds each year.

In 2004 the Patent Office launched its “IP Crime Strategy”, recognising the damage that piracy was causing to UK creative industry. Lord Sainsbury, the Parliamentary Under Secretary of State for Science and Innovation, observed in his foreword to the IP Crime Strategy that *“if we want to continue to enjoy the fruits of creativity we have to ensure that the creators can make a living and get appropriate reward for their efforts”*<sup>3</sup>. Consistent with this message, Patricia Hewitt, (the then) Secretary of State for Trade and Industry, stated *“without IP protection, the creative sector could not exist, let alone prosper. ... Government has a key role to play in protecting those intellectual property rights that provide the infrastructure for our creative economy... In the future, a strong, effective intellectual property regime will be a competitive advantage for the UK and could help make this country the location of choice for innovation and creativity”*. Ms Hewitt also added *“it is estimated that 7% of all world trade is in counterfeit goods, and that the*

<sup>1</sup> Directive on Measures and Procedures to Ensure Enforcement of Intellectual Property Rights

<sup>2</sup> A copy of this Report is available for download at <http://www.bsa.org/globalstudy/>

<sup>3</sup> See <http://www.patent.gov.uk/about/enforcement/ipbook.pdf>

*EU has lost over 100,000 jobs in the last 10 years because of counterfeit and pirated products ... we cannot and we will not tolerate this*<sup>4</sup>.

The importance of creative industry to the UK economy has also been reflected in the launching of the Creative Industries Forum on Intellectual Property. This cross government body was formed to examine both the opportunities for, and threats to, UK creative industry: in so doing, it has recognised that piracy poses a serious threat to UK creative industry. It tasked a working group, the Intellectual Property Crime and Online Infringements Group (the “IPCOI Working Group”), to produce recommendations on enforcement related matters concerning piracy. These Recommendations were finalised in February 2005 and are referred to in this document as the “IPCOI Recommendations”.

Levels of piracy are directly related to the ability of intellectual property rights owners to combat such piracy. Weak enforcement measures and remedies contribute to hugely damaging levels of piracy. The Enforcement Directive is intended to provide means by which EU member states can create, implement and expand existing procedures and remedies relating to the enforcement of intellectual property rights, that will enable piracy to be properly dealt with.

There are 2 key provisions of the Enforcement Directive which the United Kingdom Government should adopt. These should be implemented to address serious deficiencies in current law and procedure, as follows:

#### **Laws on Damages Must be Amended (Article 13)**

Damages are awarded to the owner of intellectual property rights if that owner’s rights have been infringed. In the United Kingdom, the basis upon which damages are awarded is wholly out of date with modern trends of intellectual property infringement, in particular, in connection with the problem of “end user” piracy.

End user piracy is the installation and/or use of software programmes without the possession of a licence. Software programmes are protected by copyright law: every installation of a software programme should be accompanied by the acquisition of a corresponding and valid licence (a “software licence”). End user piracy is a widespread phenomenon, and takes place within commercial organisations such as businesses, as well as publicly funded organisations such as Government departments, schools and universities. Schedule 1 to this Paper illustrates how end-user piracy can arise.

UK damages laws do not comply with Article 3 (2) of the Enforcement Directive, which requires that such remedies shall be “effective, proportionate and dissuasive”. This echoes the requirements of Article 41 (1) of the TRIPS Agreement<sup>5</sup>, which requires that such remedies should “constitute a deterrent to further infringements”. Current damages laws do not constitute any deterrent or dissuasive factor in respect of end user piracy, as evidenced by the large rate of piracy in the UK and the attendant piracy related losses suffered by the software industry in the UK. Schedule 1 explains how this lack of deterrent is an entrenched feature of damages law in the UK.

<sup>4</sup> Speech to City Group: “Creativity in the Knowledge Economy”, June 29th 2004.

<sup>5</sup> Agreement on Trade Related Aspects of Intellectual Property Rights, 1994

The problem is not confined to end user piracy. In its Key Recommendations, the IPCOI Working Group found that *“the experience of right owners is that the monetary awards made by the courts - in the form of damages or an account of profits - do not provide adequate compensation or in particular adequate deterrent”*, and that *“the Copyright, Designs and Patents Act 1988 should therefore be reviewed so that in practice damages awarded constitute a genuine deterrent to infringement, whether this is achieved by statutory change, judicial guidance or otherwise”*. BSA supports and echoes this view.

**BSA recommends that amendments to current damages laws be introduced pursuant to Articles 13(1)(a) and (b) of the Enforcement Directive. This is an ideal opportunity for the UK Government to introduce long needed reform.**

### **Civil Search and Seizure Orders Should be Readily Available and Effective (Article 7)**

Software products are very easy to delete, and so the evidence of the illegal use, supply or manufacture of software is equally easy to destroy. BSA members therefore have difficulty in identifying, seizing and preserving evidence of piracy, without gaining access to the premises of users that they suspect of such piracy. This access and seizure can be gained through the granting of a “civil search and seizure order”.

BSA members have largely been unable to utilise this remedy in the United Kingdom (and certain other EU member states) because of the onerous procedural burdens placed upon them. The information that BSA members would wish to use in such a civil search and seizure application will frequently come from persons that have some form of relationship with the “target” of that application (for example, former employees) who are concerned that acts of piracy may be taking place. However, BSA is effectively precluded from using this evidence. This is because it must provide the source of the evidence - that is, the witness’s identity - to their intended target. Schedule 2 to this Paper explains why this is the case.

For social, employment and, on occasion, personal safety reasons, BSA believes that the identity of such persons should be protected. This is the position in the Republic of Ireland, and in several other EU Member States. This is not the position in the United Kingdom. BSA members are denied access to the civil search and seizure remedy because they must identify the source of their information in all civil search and seizure applications. This is contrary to the interests of justice.

This is a conclusion shared by the IPCOI Working Group. It has recommended that the *“Government should explore the possibility of enhancing the possible response from the court to an IP infringement where at least some of the evidence has been provided by a person who has legitimate reasons for not wanting their name to be disclosed. In particular the Government should address the position of whistleblowers by assuring them of confidentiality where they have a genuine fear of the consequences should their name become known by the alleged infringer.”*

In addition, the cost and complexity of the civil search and seizure remedy in the United Kingdom is a serious area of concern. Such cost and complexity means that only the most wealthy of right holders can use it, and prejudices small right holders, especially when faced with attacks upon their rights by larger, wealthier organisations.

The complexity and expense of the civil search and seizure measure is exacerbated by the “supervising solicitor” requirement. The role of a supervising solicitor is to ensure, as far as possible, that the conduct of a civil search and seizure action takes place within the limits set by the Court. This is a superfluous role, because the conduct of the search and seizure is conducted

by Officers of the Court, who have a duty to the Court to ensure that the Order is correctly complied with. The sanctions applied to parties and practitioners for unauthorised or excessive conduct are severe: the supervising solicitor role is thus an expensive anachronism.

**In Summary:**

- **Article 3 of the Enforcement Directive requires that procedures covered by that Directive (including the civil search and seizure remedy) should not be “unnecessarily complicated or costly” - BSA believes that the civil search and seizure remedy is both unnecessarily complex and expensive, and should be reformed.**
- **Article 7(5) of the Enforcement Directive allows Member States to provide for the protection of witness evidence in such cases. BSA encourages implementation of this provision, and Schedule 2 to this Paper suggests an implementation path in this regard.**

## **About Business Software Alliance**

The Business Software Alliance ([www.bsa.org](http://www.bsa.org)) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce. BSA members include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, Cadence Design Systems, Cisco Systems, CNC Software/Mastercam, Dell, Entrust, HP, IBM, Intel, Internet Security Systems, Macromedia, McAfee, Microsoft, PTC, RSA Security, SAP, SolidWorks, Sybase, Symantec, Synopsys, The MathWorks, and UGS.

For further information regarding BSA, or this Paper, please contact:

Francisco Mingorance,  
Director Public Policy,  
BSA Europe.  
Tel: +32 (0)2 401 6808  
e-mail : [franciscom@bsa.org](mailto:franciscom@bsa.org)

## **Schedule 1: Deficiencies in UK Damages Laws**

- 1.1 Business Software Alliance members are creators and suppliers of software. Software products are protected by copyright law, and so using computer software products is unlawful unless the user has a licence from the relevant software publisher. These licences are supplied by computer software producers and suppliers, and are generally referred to as “software licenses”. In the business context, using software without software licences is referred to as “end user piracy”.
- 1.2 BSA members suffer from a worldwide problem in respect of end user piracy. End user piracy can arise from a variety of sources: users deliberately install software without licences through a variety of means, including the over use and installation of a small number of legitimate software products, the installation and use of pirated software, and the use of “cracked” software, for example when legitimate software with some technological restriction (such as a time lock or user lock) is circumvented by the use of illicit circumvention techniques.
- 1.3 End user piracy causes huge revenue losses to the software industry in the United Kingdom. These losses, and the fact that end user piracy is so widespread, are directly related to the fact that the law on damages relating to end user piracy is out of date and wholly inadequate. In end user piracy cases, guilty parties invariably seek to resolve matters by acquiring software licences for the software programmes they have been using without licences. They then argue that the fact they have purchased licences for the software they were using without licences eliminates any obligation to pay damages or costs.
- 1.4 BSA believes that the majority of end user piracy takes place in the knowledge that the “worst case scenario” for such users is that, if identified as being “guilty” of end user piracy, all that will be required is a licence purchase. This type of “risk assessment” contributes heavily to the high rates of piracy in the United Kingdom, and is a root cause of the financial losses suffered by the software industry in the United Kingdom.
- 1.5 Although Section 97 (2) of the Copyright, Designs and Patents Act 1988 provides an “additional damages” remedy for rightholders, BSA agrees with the conclusion of the IPCOI Working Group, in that the manner in which the section has “*been applied in practice by the courts has not sufficiently reflected the gravity of the infringements in issue in the scale of the additional damages awarded*”. BSA believes that a remedy analogous to that which provides for deterrent levels of damages in the form of minimum statutory damages (such as in the United States and Canada), multiple damages (such as in Lithuania, Poland and Greece) or exemplary damages (such as Japan and Australia), would be appropriate: and notes that a wide ranging remedy providing for judicial discretion for damages awards exists in Ireland.

## **Schedule 2: Deficiencies in UK Civil Search and Seizure Procedures**

### **The Current Restrictions**

Section 7 of the Civil Procedure Act 1997 (the “Act”) provides a statutory basis for Courts to make an order to secure either the “*preservation of evidence which is or may be relevant*” or “*the preservation of property which is or may be the subject-matter of the proceedings.*” The relevant Civil Procedures that deal with how these orders should be made are contained in Civil Procedure Rule 25 (“CPR 25”) and the accompanying Practice Direction (“PD 25”). These provisions do not state whether information from an anonymous source may be used as the basis for granting a search order. Common law has, however, developed in a manner that prevents the use of information from anonymous sources.

In the *WEA Records*<sup>6</sup> case, the Court stated that it is not right for a judge to hear confidential information which cannot be disclosed to the defendants at a later stage. The issue only should be considered based on the evidence known to both parties. Consequently, where a judge is given anonymous evidence, he must ignore it. The Court said it could not “... *visualise any circumstances in which it would be right to give a judge information... which cannot at a later stage be revealed to the party affected by the result of the application.*”

In the *Gadget Shop*<sup>7</sup> case, the defendant tried to overturn an order that had been granted on the grounds that the claimant had failed to disclose everything it should have done to the judge when it applied for civil search order. The Court agreed that there was a duty to make full, frank and accurate disclosure of all “material information”: it is clear that the identity of a witness in such a case would constitute “material information”.

### **Justification for Change**

#### **(i) interests of justice**

It is in the interests of justice for witnesses to feel confident and secure in providing evidence that relates to the infringement of their intellectual property rights. It is also in the interests of justice for rightholders to be able to use that evidence, if necessary in civil search and seizure proceedings, without restriction. The outdated and obstructive bar to “anonymous” evidence in civil search and seizure applications should be removed. Judges in applications will still retain absolute discretion whether or not to grant such orders based on such evidence, and Defendants will be protected by the current rules relating to Claimants’ providing undertakings as to damages to compensate the Defendant if they are mistaken.

#### **(ii) international precedent**

Several European jurisdictions permit the granting of civil search and seizure applications based upon anonymous evidence, including Sweden, Denmark, Finland, France, Belgium and Spain.

<sup>6</sup> *WEA Records Ltd v Visions Channel 4 Ltd* [1983] 2 All ER 589

<sup>7</sup> *Gadget Shop Ltd v Bug.Com Ltd* [2001] FSR 383

The United Kingdom's nearest neighbour, Ireland, has an ideal provision in respect of the use of such evidence. Section 132 of the Copyright and Related Rights Act 2000 provides as follows:

- (3) In ... any ex parte application... to a Court ... for an order which would permit the applicant to enter and search premises ... and take possession of material ... the Court hearing such an application may receive hearsay evidence to the effect that the witness or deponent believes that the material may be found in a particular location
- (4) A witness or deponent shall not be obliged to indicate the source of the information upon which that witness formed the belief the material may be found in a particular location.

### **(iii) domestic precedent**

There are examples of how such “anonymous” evidence has been admitted in civil proceedings in England and Wales, without there having been deemed to be any adverse risk to the interests of justice being served.

In a public law case, *Re W*<sup>8</sup>, the court held that it was a matter for the judge's discretion on whether evidence should be provided anonymously. In determining whether anonymous evidence should be permitted, the judge balanced the need for protection against any unfairness or prejudice. Further, in a separate case,<sup>9</sup> the headmaster of a school made reference to an anonymous statement provided by a pupil. The defendant claimed that this was unfair. The Court dismissed the appeal, noting that the claimant had been allowed to question the headmaster concerning the evidence, making the identification of the pupil superfluous.

### **(iv) process efficiency**

In its Consultation Paper regarding the Enforcement Directive, the Patent Office has indicated that it believes that Rule 39.2 of the CPR does allow a Court to order that the identity of any party or witness must not be disclosed if it considers non-disclosure necessary in order to protect the interests of that party or witness. It appears that the Patent Office believes that this provision applies to civil search and seizure applications. This is not the view of the BSA. However, if it is the belief of the Patent Office (and the Department of Constitutional Affairs) that CPR 39.2 is intended to protect the identity of witnesses from disclosure in civil search and seizure applications, BSA suggests that a simple clarifying amendment to the CPR is all that is necessary in this regard.

<sup>8</sup> [2002] EWCA Civ 1626

<sup>9</sup> *R (on the application of A) v Westminster City Council* [2002] EWHC 2351