ATTACHMENT

Platform Transparency in the Digital Single Market

It is an elementary principle of both physical commerce and e-commerce that service providers should identify themselves. For dozens of everyday reasons such as lodging complaints, requesting refunds, making claims, or complying with legal requirements, consumers and other businesses have a reasonable need to know with whom they are dealing.

Such transparency is a long standing cornerstone in all forms of commerce, and Article 5 of the E-Commerce Directive (ECD) embodies this principle in the online world by requiring information society service providers to clearly indicate their identity. In its October 2012 Report on Completing the Digital Single Market, **the European Parliament recalled that "compliance with this requirement is vital to ensuring consumer confidence in e-commerce[1]"** while, in the communication welcoming the final adoption of the ECD the Commission specifically reminds that the transparency requirements apply to:

> *on-line newspapers, on-line databases, on-line financial services, on-line professional services (such as lawyers, doctors, accountants, estate agents),* ***on-line entertainment services such as video on demand****, on-line direct marketing and advertising and services providing access to the World Wide Web.*[2]

The transparency requirements were also intended to allow authorities to determine in which member state the service is based so as to apply the relevant (tax) regulations.[3] Unfortunately, illegitimate service providers routinely ignore Article 5 ECD with impunity, wilfully hiding their identity. They do this because operators who are seeking to infect consumers' computers with malware, commit fraud, infringe rights of privacy or property, avoid paying taxes, or otherwise violate the law naturally prefer to remain anonymous.

By contrast, compliance with Article 5 by legitimate VOD platforms is not a problem, inasmuch as the Directive requires the disclosure of basic information only: name, address, e-mail address, trade register number, professional authorisation and membership of professional bodies where applicable and VAT numbers. Its requirements are therefore easily met by legitimate platforms.

Unfortunately these legitimate operators have their businesses undermined by shadowy actors who run substantial illegal online enterprises (websites and apps) generating millions of pounds in revenue in complete anonymity, hiding behind fraudulent contact information.

---

[1] The European Parliament's Legal Affairs committee confirmed this view in its opinion on the European Parliament's report on the Digital Single Market adopted on 3 December 2015. (*27.Recalls that pursuant to Article 5 of Directive 2000/31/EC, providers of online services are obliged to clearly indicate their identity, and that compliance with this requirement is vital to ensuring consumer confidence in e-commerce*). Furthermore, the European People's Party adopted a position paper on copyright on 18 November 2015 that states that "*the EPP Group also supports initiatives aimed at improving the transparency of online platforms and at encouraging search engines to guide consumers towards legal content online*".

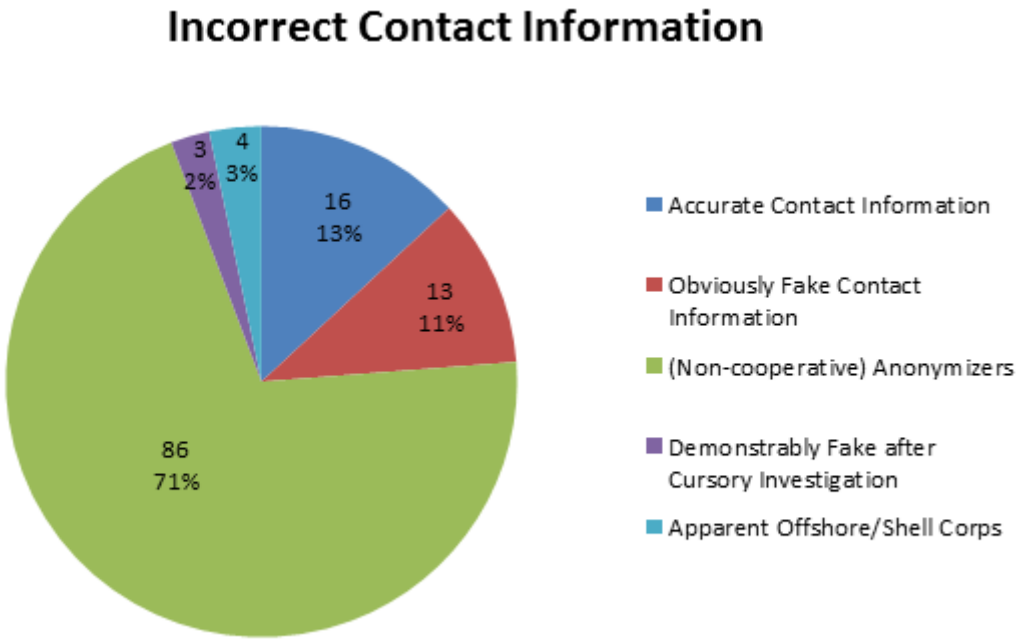
[2] Ref: http://europa.eu/rapid/press-release_IP-00-442_en.htm?locale=nl (emphasis added).

[3] Ref: http://europa.eu/rapid/press-release_IP-98-999_en.htm?locale=nl

Following successful criminal and civil prosecutions in the UK against sites such as SurfTheChannel and Newzbin, the top level illegal websites (scoring Alexa rankings in the UK on par with sites such as the BBC, Guardian, Booking.com, etc) are only too aware of the possibility of jail sentences and damages handed out by the courts. In reaction these sites have gone to great lengths to protect their identities, for example by setting up fake shell companies on exotic islands.

Below the top-tier infringing websites sit a large number of mid/low tier websites that may lack the means to set up sophisticated corporate veils and instead use privacy protect services or register entirely false identities, sometimes using dreamt-up names or randomly stealing identities from the telephone directory. Payments are often made by pre-paid credit cards and digital currencies like bitcoin, etc. In order to stay online, these sites will, using a fake identity, conclude a contract with a hosting provider, register a domain name and, in order to generate revenue, contract with an advertising broker and payment provider for premium subscription models and/or donations.

MPA's expertise in this area specifically pertains to websites that engage in commercial-scale infringement of copyright in motion pictures and television programmes. MPA's analysis of a group of 122 sites of concern in that regard in Europe between 2013 and 2015 indicates that only a small minority (13%) of suspect sites listed contact information that appeared likely to be accurate in publicly accessible "WHOIS" databases, while the other 87% hid their identities.



Source: MPA Analysis of 122 Sites of Concern to MPA Members, 2013-2015

Most of the sites MPA analysed (71%) used publicly available anonymisation services, such as Whoisguard Inc. and Privacy Protection Service Inc., which advertise themselves as a way for individuals registering domain names to protect themselves from spammers. In the case of commercial information society services providers, however, use of such a service tends to indicate that the service provider is choosing not to comply with Article 5 ECD. (While WHOIS data is not the only means by which sites can disclose the information required by

Article 5 ECD, MPA has found that commercial infringement sites that go to the trouble to hide their identities from the WHOIS database do not, as a practical matter, disclose their identities on their sites or in other ways that would be "easily, directly and permanently accessible" as the Directive requires.)

Other sites MPA analysed (11%) listed obviously fake contact information, such as the following information listed for the site piratestreaming2.com:

```
Registry Registrant ID:
Registrant Name: nikoj nikoj
Registrant Organization:
Registrant Street: nikoj
Registrant City: nikoj
Registrant State/Province: nikoj
Registrant Postal Code: 1530
Registrant Country: Macedonia
Registrant Phone: +389.75000000
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: piratestreaming2@gmail.com
```

A few sites (5%) listed information from apparent offshore/shell companies, or information that proved to be fake after only a few minutes of investigation.

<u>The policy implications of widespread non-compliance with Article 5 are serious, particularly but not exclusively for rights holders</u> : While the data above are focused on the audiovisual sector, where our experience lies and the problem is acute as to illegal sites, investigations by Member State consumer protection authorities have found the problem to exist in other areas as well. The ability to operate anonymously online undermines the rule of law in fields such as consumer protection, privacy, and taxation – to name just a few – and enables online criminal activity.

For rights holders in particular, unsanctioned noncompliance with Article 5 ECD creates structural enforcement issues. For example, non-compliance with Article 5 ECD cascades down the enforcement tree by rendering the Right of Information remedy in Article 8 of the Enforcement Directive inutile. Rightholders have in fact obtained a number of pyrrhic victories against Internet service providers to render account of the identities of their infringing customers (website operators) since, following lengthy and costly court proceedings, the obtained contact details in almost all cases proved to be false or unhelpful.[4]

Possible regulatory changes to enhance transparency

The digital single market strategy and related initiatives provide a key opportunity to open a conversation about how to ensure that the existing transparency rules in the ECD are better respected. The protection of consumers and of the most vulnerable (including children) should clearly be central considerations in that process. [5] In addition to those

[4] Ref Lycos/Pessers (Dutch Supreme Court) / Ref MPA/Black Internet (Swedish CoA) &ors.

[5] In addition to the other issues at play, we also highlight the privacy concerns this causes. Internet intermediaries are under the same obligations as any other data processor in having to ensure that the records

considerations, we would urge careful consideration of the economic and rule of law interests harmed by non-compliance with Article 5, including those of creators and their business partners.

We therefore propose that the responsible EU and Member State authorities use their ongoing consultation processes under the DSM umbrella to explore how to make the transparency requirement in Article 5 ECD more meaningful by attaching proactive measures that must be taken to aid in ensuring the accuracy of identifying information provided as well as dissuasive consequences for failure to comply, while making reasonable allowances for honest mistakes by legitimate operators. We do not prejudge at this early stage what type of proactive measures or consequences would be most appropriate, or what type of measure is needed to embody them, but look forward to discussing those and other questions further in the context of a multi-stakeholder process.

Critically, the negative impact of these transparency improvements would, by design, fall on illegitimate operators who refuse to meet even the most basic minimum standard of transparency required to do business in the EU. Imposing serious consequences on those operators will helpfully sharpen distinctions between legal and illegal operators, which will strengthen the legitimate digital single market.

---

they keep are correct. The inaccurate record keeping practices allow criminals to leverage the identity theft to commit a variety of crimes shielded by unwitting citizens.