The Dickson Poon
School of Law

BLACKLISTING: A NEW EFFECTIVE DIGITAL TOOL AGAINST COUNTERFEIT SALES ONLINE (LEGAL OPINION)

D. Chernysh

BLACKLISTING: A NEW EFFECTIVE DIGITAL TOOL AGAINST COUNTERFEIT SALES ONLINE (LEGAL OPINION)[1]

TABLE OF CONTENTS

[1] I would like to extend my deep and sincere gratitude to my supervisor Professor Frederick Mostert for his valuable support, constructive feedback, expert guidance, and perhaps most of all his general patience with me.

I. INTRODUCTION

In a technology-driven world, the models of conducting business by the rightsholders and online intermediaries (**"Good Actors"**) are changing frequently to adapt new demands of consumers and to improve the speed and quality of services, so too are the behaviour patterns of the counterfeiters and pirates (**"Bad Actors"**), who adjust instantly to cutting-edge technologies for committing their illegal actions. This has encouraged Good Actors to look for new more effective means for tracking and tracing Bad Actors and curbing online infringements.

This Legal Opinion (**"Legal Opinion"**) focuses on introduction of a "blacklisting" digital tool as a newly developed solution for fighting against increasing sales of counterfeits in the digital environment, as well as for preventing Bad Actors from other violations of intellectual property rights (**"IPRs"**), such as copyright infringement and intentional misappropriation of intellectual property (**"IP"**). This solution is based on a comprehensive study and analysis of the global picture and statistics of counterfeit sales, with a primary focus on the online market, along with the current approaches, methods and instruments used to restrain the growing numbers of pirated and counterfeit goods. Moreover, the paper proposes a "blacklisting" classification, which may serve as "a traffic light system" to tackle the online infringements[2], and describes its step-by-step implementation process.

The Legal Opinion is divided into four main parts. The first part will describe a set of global problems resulting from illegal activities of Bad Actors, and critically analyse the existing ways to solve them; it will also provide a recent review of official reports by national and international authorities about world counterfeiting tendencies and statistics. The second part will suggest the definition of the "blacklisting", outline its main characteristics, and offer the possibilities of its integration into the commercial environment. The third chapter will seek to critically evaluate the use of the "blacklisting" tool within the existing legal framework and propose the consequent changes to the existing laws. And, finally, the conclusion will summarise all the above information on how the current and future role of the "blacklisting" fit in the digital environment.

---

[2] Interview with Weizmann Jacobs, Detective Constable, Police Intellectual Property Crime Unit (**"PIPCU"**), the City of London Police (King's College London, 14 November 2018).

The research on this particular subject is comprised of a number of publicly available working papers, peer-reviewed published articles and practical information based on the expertise and experience of competitive authorities and business community involved in creation and implication of up-to-date solutions for fighting against online IP infringements.

II. PREREQUISITES TO CREATION OF BLACKLISTING TOOL

II. 1. GLOBAL PROBLEMS AND CURRENT TENDENCIES IN COUNTERFEITING INDUSTRY

Global intellectual property theft and prevalence of pirated and counterfeit goods continue to grow at alarming proportions, creating an inevitable threat to economies and businesses worldwide, resulting in income losses, decrease in tax revenues and disruption of the investment climate. Apart from this, counterfeits pose big risks to the welfare of customers and negatively influence most of the social sectors[3]. Public health *inter alia* remains of the greatest importance due to the high volume of substandard and falsified pharmaceuticals[4] and baby products[5]. In addition, the money received from sales of counterfeits supports child pornography, forced labour, terrorism and other criminal activities which undermine moral stance, privacy and security of the whole society[6].

In recent times the issue with counterfeits and IP theft has also led to a serious international conflict between two major trading partners - China and USA, that consequently disrupts commercial relations between two states and undermines worldwide economy[7].

---

3 Counterfeiters deprive the public sector of tax revenue which supports public schools, hospitals and other social organisations; and with the lack of financial support, citizens cannot receive social services essential for their well-being.

4 The World Health Organization (**"WHO"**) confirms that 1 in 10 medical products in low- and middle-income countries are counterfeits - WHO, 'Substandard and falsified medical products' (31 January 2018) <https://www.who.int/en/news-room/fact-sheets/detail/substandard-and-falsified-medical-products> accessed 15 July 2019.

5 Organisation for Economic Co-operation and Development (**"OECD"**) and European Union Intellectual Property Office (**"EUIPO"**), *Trends in Trade in Counterfeit and Pirated Goods, Illicit Trade*, (2019 OECD/EUIPO Report, Paris, 2019), 59.

6 The International Anticounterfeiting Coalition, *Counterfeiting costs everyone* <https://www.iacc.org/resources/about/what-is-counterfeiting> accessed 15 August 2019.

7 Jeanna Smialek, Jim Tankersley and Jack Ewing, 'Global Economic Growth Is Already Slowing. The U.S. Trade War Is Making It Worse' (18 June 2018) N.Y. Times <https://www.nytimes.com/2019/06/18/business/economy/global-economy-trade-war.html> accessed 8 July 2019.

One of the reasons why the counterfeiting industry keeps thriving is the constantly changing patterns of Bad Actors' behaviour due to the development of new technologies and evolved methods of sales and distribution. Besides that, Bad Actors are often more sophisticated in using high-tech opportunities for copying the existing business models of Good Actors and refining the digital processes.

The problem exacerbates when Bad Actors start imitating each construction and appearance detail of the genuine products[8] that make counterfeits more indistinguishable from them. And the invention of 3-D printing technology further increases the related risks[9].

Additionally, the lack of due identification and verification of Internet users has made it easier for Bad Actors to avoid detection. Subsequently, the users can instantly create online accounts in social networks or open online shops and just as quickly close them down to avoid exposure, if they attract enforcement bodies[10]. Therefore, ease of opening and shutting down businesses, speed of distribution and anonymity have created a favourable environment for Bad Actors to proliferate their illegal business.

As highlighted in the European Union Serious and Organised Crime Threat Assessment 2017 (**"SOCTA 2017"**), in the recent time counterfeiting is expanding sufficiently its reach on online marketplaces[11], and, in particular, on major social media platforms[12]. For example, Instagram has become the most attractive platform for bad actors with 56,769 active counterfeit accounts in 2018, which is more than 171% when compared to 20,892 accounts in 2015[13]. This also results in a serious shift from business-to-business (B2B) to business-to-consumer (B2C) model. And the logical consequence of this is the tendency of trafficking counterfeits in small parcels via postal or express services[14]. And although counterfeits

---

8 Thomas J. McCarthy, *Trademarks and Unfair Competition* (4th ed., 2014) §25:10.

9 Joelle Bergeron, '*Working document on three-dimensional printing, a challenge in the fields of intellectual property rights and civil liability'*, Committee on Legal Affairs of European Parliament (23 November 2017) 3.

10 Frederick Mostert, 'Study On Approaches To Online Trademark Infringements' (1 September 2017) WIPO/ACE/12/9 REV. 2, §5.

11 Europol, *'SOCTA: EU Serious and Organised Crime Threat Assessment, Publications Office of the European Union'*, (Luxembourg, 2017).

12 Andrea Stroppa, Davide Gatto, Lev Pasha and Bernardo Parrella, '*Instagram and counterfeiting in 2019: new features, old problems*' (9 April 2019) 10.

13 ibid 41.

14 2019 OECD/EUIPO Report (n 5) 19.

distributed by container ships prevail in terms of value, trafficking of fake goods by small parcels is growing and dominate in a number of seizures[15].

These recently evolved tendencies, backed by current statistics below, serve as an undisputable prove of Bad Actor's prosperity on the global market.

II. 2. UP-TO-DATE STATISTICS

Low overhead expenses and instant high revenues make counterfeiting business attractive to a larger number of existing or potential Bad Actors. This is also proved by a summary of up-to-date statistics which reveal the existing scale of counterfeits as well as forecast the future figures.

The Global Brand Counterfeiting Report 2018-2020 (**"GBCR"**) estimates the amount of total counterfeiting globally having reached 1.2 Trillion USD in 2017, including $323 Billion of losses from online counterfeiting, with a forecast up to $1.82 Trillion by the year 2020[16]. In the INTA and BASCAP Report, the figures echo the picture presented by GBCR, projecting the increase of fake goods for 2022 up to between $1.9 - 2.81 Trillion[17].

Moving to the regional level, trade in counterfeit and pirated goods in the EU stands at 6.8% of EU imports from third countries[18]. In particular, the European Commission reveals a number of more than 31 million articles suspected of violating intellectual property rights[19]. In the same year, the EU Customs registered almost 60.000 detention cases with the total value of the detained articles, had they been genuine, to be over €580 million[20].

---

15 OECD/EUIPO, '*Misuse of Small Parcels for Trade in Counterfeit Goods: Facts and Trends'*, (OECD Publishing, Paris, 2018) 77.

16 See Global Brand Counterfeiting Report, 2018 (R Strategic Global, December 2017).

17 Frontier Economics, *'The Economic Impacts of Counterfeiting and Piracy'* (Report prepared for BASCAP and INTA, February 2017) 56.

18 2019 OECD/EUIPO Report (n 5).

19 European Commission, *'Report on the EU customs enforcement of intellectual property rights. Results at the EU border'* (2018) 6.

20 ibid

At national levels, the intensity of counterfeiting and piracy is also rising. In the UK, PIPCU has disrupted £719 million worth of IP crime since 2013[21]. Whilst in the U.S., Customs Border Protection Report discloses the total estimated manufacturer's suggested retail price (MSRP) of the seized goods as $1,206,382,219 [22]. In the digital piracy context, the U.S. economy loses $ 30 billion annually as a consequence of copyright theft[23].

China and Hong Kong remain the main sources of counterfeits spreading to the above countries and across the globe[24], having been the provenance of 86 % of global counterfeiting and USD 396.5 billion worth of counterfeit products in 2015[25].

Consequently, the intensity of counterfeiting and piracy is on the rise, with significant potential for IP theft in a globalised economy[26].

II. 3. EXISTING APPROACHES, METHODS AND SOLUTIONS TO TACKLE ONLINE INFRINGEMENTS

Notwithstanding the formidable magnitude and abundance of the problem, online counterfeits and digital piracy are relatively new IP crimes, having been evolved in the past years due to technology and specific functionality of the Internet. As a result of both factors, it has become impossible to restrain the unfettered growth of online counterfeits by traditional mechanisms which have many limitations and are not adequately adapted to deal with online infringements[27].

---

[21] 'PIPCU disrupts £719 million worth of IP crime' (Press Release, 21 January 2019) <http://news.cityoflondon.police.uk/r/1184/pipcu_disrupts__719_million_worth_of_ip_crime> accessed 4 June 2019.

[22] U.S. Customs and Border Protection Office of Trade, '*Intellectual Property Rights, Fiscal year 2017 Seizure Statistics* (2017) <https://www.cbp.gov/sites/default/files/assets/documents/2019-Apr/FY%202017%20Seizure%20Stats%20Booklet%20-%20508%20Compliant.pdf> accessed 13 July 2019, 6.

[23] David Blackburn, Jeffrey A. Eisenach and David Harrison Jr., 'Impacts of Digital Video Piracy on the U.S. Economy' (June 2019) < https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf> accessed 26 August 2019.

[24] EUROPOL/EUIPO, '2017 Situation Report on Counterfeiting and Piracy in the European Union' (2017), 7.

[25] US Chamber of Commerce, '*Measuring the magnitude of global counterfeiting: creation of a contemporary global measure of physical counterfeiting'* (Washington DC, 2016), <https://www.uschamber.com/sites/default/files/documents/files/measuringthemagnitudeofglobalcounterfeiting.pdf> accessed 16 June 2019, 3.

[26] 2019 OECD/EUIPO Report (n 5).

[27] Frederick Mostert, 'Study on IP Enforcement Measures, Especially Anti-Piracy Measures in The Digital Environment' (3 July 2019) WIPO/ACE/14/7, 23.

Due to the length and expensiveness of trials civil litigation remains beneficial only in large-scale cases with persistent infringers[28]. Moreover, the process is tangled by the lack of possibility to detect those involved in IP crime since the criminals use fake accounts and IDs, multiple phone numbers, ciphering systems and other illicit methods to keep their animosity. Criminal prosecution can be a cost-effective alternative to civil enforcement, however, due to budget, time and capacity constraints of law-enforcement authorities[29], the burden of collecting the evidence sufficient to start investigation will fully lie on the claimant. Moreover, in some jurisdictions, a counterfeit case will be initiated only if it surpasses a specific value or volume threshold[30]. Considering this as well as territorial limits, both civil and criminal enforcement ways can be used in exceptional cases.

The legislators also try to hold back the counterfeiting growth; however, their attempts usually fall far behind the commercial and technology developments used by both traders and counterfeiters[31].

As a result, IP stakeholders and intermediaries have started searching for and creating new methods, more practical and viable, to restrain unfettered growth of counterfeits both nationwide and worldwide.

As of today, digital technology is recognised as the central element in combating online piracy and preventing dissemination of counterfeit products in the global net. All market players are continuously working on creation and implementation of various digital tools and software solutions to tackle the infringements, whilst the government encourages and supports investments in this field[32].

---

[28] Annual costs for IP Litigation, in general, have increased from USD 1.7 billion in 2005 to USD 3.3 billion in 2019 - see Morrison & Foerster, 'Preparing for the Increased Globalization of IP Litigation' (Study, 7 August 2019) <https://mofotech.mofo.com/topics/preparing-increased-globalization-ip-litigation.html> accessed 10 August 2019.

[29] Julia Dickenson, Jason Raeburn Katrina Thomson, 'Procedures and strategies for anti-counterfeiting: United Kingdom' (14 May 2019) *World Trademark Review* <https://www.worldtrademarkreview.com/anti-counterfeiting/procedures-and-strategies-anti-counterfeiting-united-kingdom-1> accessed 14 July 2019.

[30] Doug Palmer, Melanie Lee, 'Special report: Faked in China: Inside the pirates' web' (26 October 2010) *Reuters* <https://www.reuters.com/article/us-china-counterfeit-idUSTRE69P1AR20101026> accessed 11 July 2019.

[31] Frederick Mostert, 'The Internet: Regulators Struggle To Balance Freedom With Risk' (*Financial Times*, 9 July 2019) <https://www.ft.com/content/e49c39e6-967d-11e9-8cfb-30c211dcd229> accessed 11 July 2019.

[32] HM Government, *Online Harms* (White Paper, April 2019) 9.

A recent solution was proposed by the Dutch inventors at Copenhagen University who created an authentication technology in the form of a chemical transparent ink fingerprint that helps to reveal identity of the product by using the app on smartphones[33]. Although this invention helps to check the authenticity of goods, once purchased, it cannot tackle online infringers who may disappear at any time. A similar idea for item identity is used by Amazon as a part of Transparency programme[34] to ensure that customers receive genuine products.

Besides the authentication tools, many popular online platforms have successfully implemented Notice and Takedown procedures under which the rightsholders notify the intermediary about an alleged infringement and the latter removes the counterfeiting products from the marketplace. However, due to the simplicity of uploading and deleting the content on the Internet, allowing the illegal product to reappear immediately, once deleted, on a different list or platform, the Notice and Takedown process does not help with the problem effectively[35]. Additionally, the massive amounts of information prevent the rightsholders from tracing each infringement case and intermediaries from reacting promptly towards multiple requests from the former[36]. This keeps a sufficient amount of cases unresolved and does not disrupt the continuous flow of counterfeits.

Other innovative solutions, such as content verification tools, monitoring and filtering mechanisms, stay down processes and disclosure procedures, have been also criticized as contradicting with existing laws on the protection of the freedom of speech, competition or data protection and being burdensome for intermediaries[37].

Therefore, some of the solutions and mechanisms can deal only with *ad hoc* situations or are territorially constrained, others require sufficient time and financial investments. All these and other limitations slow down the process of fighting counterfeit sales online. For this reason, the demand for new and more sophisticated tools in the digital world has become sharp.

---

[33] University of Copenhagen, 'New weapon to combat counterfeit goods: use your smartphone to check for fake merchandise' (Science Daily, 21 February 2019) <https://www.sciencedaily.com/releases/2019/02/190221111717.htm> accessed 1 June 2019.

[34] See Transparency <https://brandservices.amazon.com/transparency> accessed 1 August 2019.

[35] Frederick Mostert (n 10)§20.

[36] ibid §21.

[37] ibid §42.

Beyond the technological tools, some realise the importance of collaboration between online platforms, governmental authorities and legislatures. In this respect, some discuss the benefits of voluntary collaboration practices (**"VCPs"**) developed by market players of different levels to establish preventive and proactive measures against online IP infringements. The best VCPs, serving as guidelines for fair trade conduct and protection of rightsholders, were analysed in a recent EUIPO study[38]. In the author's opinion, enhanced cooperation and coordination is essential for success in fighting against counterfeits and, as it will be shown further, forms a formidable basis for the "blacklisting" tool.

III. INTRODUCTION TO THE BLACKLISTING DIGITAL TOOL

III. 1. OVERVIEW

The proposal to create universal digital mechanisms which could help to prevent counterfeits and IP theft globally has been widely discussed by both academic and business communities in the recent days[39]. As part of an overall solution, some representatives of the industry and public authorities have proposed the creation of "blacklists"[40], aimed at tracking down and blocking the repeated infringers.

In general terms, "blacklisting" is a ban, embargo on certain actions or a limit of access to some resources or people. Also, it may refer to lists and databases of untrustworthy actors, ranging from individuals to countries.

The "blacklisting" has been already integrated successfully into different systems and used by governmental authorities as well as online intermediaries to stop IP infringements at different levels.

---

[38] Thomas Hoeren, Guido Westkamp, María Vidal, Susana Rodriguez Ballano, Paula Iun, Ana De Lluc Compte, Jaime Pascual, Andrea Sánchez Guarido and Julia Torres, 'Study on Voluntary Collaboration Practices in Addressing Online Infringements of Trade Mark Rights, Design Rights, Copyright and Rights Related to Copyright' (September 2016), *EUIPO* <https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Research%20and%20sudies/study_voluntary_collaboration_practices_en.pdf> accessed 1 August 2019.

[39] Frederick Mostert (n 31).

[40] In the literature, they can be named "delists", "blocking lists", "banned lists" or "bad actor lists". All of them are synonyms of "blacklists" in this context.

At the international level, the "blacklisting" has been used as a political tool by the US government for preventing Chinese companies from misappropriation of IP and distribution of counterfeiting goods on the territory of the USA. Apart from banning the companies from trading in the territory of the USA, the newly introduced bill seeks to enable the federal government to prevent companies on a U.S. government trade "blacklist" from buying, selling or exclusively licensing U.S. patents[41].

Moving to a country level, it's worth mentioning China as a pioneer in creating and integrating the "blacklisting" system nationwide as part of a controversial "social credit system". In the framework of this system on 21 November 2018, the Chinese National Development and Reform Commission ("NDRC") introduced a Memorandum of Cooperation on Joint Disciplinary Actions Against Seriously Untrustworthy Parties in the Field of Intellectual Property Rights, focusing on patent- and trade secret- related repeated offences, such as "irregular patent application activities" or unauthorised use of invention without the rightsholder's consent. Among the punishment for "blacklisted" infringers, the Memorandum suggests restrictions on advertising, issuing corporate bonds, obtaining financial support, participating in government procurement; lowering of one's enterprise credit rating and others[42].

The "blacklisting" mechanism is also successfully used by some governmental authorities. For example, PIPCU maintains and controls the Infringing Website List (IWL), a "blacklist" of websites accused of facilitating copyright infringement. Similar to this, the Russian Federal Service for Supervision of Communications, Information Technology and Mass Media (**"Roskomnadzor"**) controls a "blacklist" database of web-sites blocked by internet service providers, known as "the single register", as part of the Anti-piracy law 2013[43] implementation process. Moreover, the Law entitled Roskomnadzor to temporarily "blacklist" web-sites sites if they do not tackle complaints about copyright infringement

[41] Sarah Krouse and Kate O'Keefe, 'Senators Introduce Bill Restricting Huawei From Buying, Selling U.S. Patents, the Wall Street Journal' (*The Wall Street Journal,* 18 July 2019) <https://www.wsj.com/articles/senators-to-introduce-bill-restricting-huawei-from-buying-selling-u-s-patents-11563463179> accessed 21 July 2019.

[42] Steven Grimes, Gino Cheng and Ya'nan Zhao, 'China Says It Will Blacklist and Sideline Repeat Intellectual Property Right Violators' (10 December 2018) *Lexology* <https://www.lexology.com/library/detail.aspx?g=a25c6c93-4624-4925-b3bf-c6bb55478d2d> accessed 31 May 2019.

[43] Federal Law No. 187-FZ of July 2, 2013 On Amending Certain Legislative Acts of The Russian Federation On Issues Of Protecting Intellectual Rights In Information- Telecommunication Networks

within three days of being notified[44]. A controversial new provision also proposed a permanent blocking (permanent "blacklisting") of the repeated infringement of copyright or related rights, if there is already an earlier decision of the Moscow City Court in force in favour of the same claimant.

Despite various examples of "blacklists" worldwide, this Legal Opinion looks at the "blacklisting" tool from a different perspective. It represents the "blacklisting" as a universal AI-driven instrument based on big data analysis, which is primarily used as a voluntary measure by online platforms in the digital environment and shared with enforcement bodies for facilitating the process of tackling infringements. From the technological standpoint, the principle of the tool lies in the development of a pattern-matching system which would detect the illegal actions and further send notifications while the pattern is recognised, subsequently, block the access once notifications exceed a permissible limit, and keep the records of the blocked person on a special list. Therefore, a digital "blacklisting" is a complex mechanism, which consists of two entwined parts – the technological measure which denies access to online services of online marketplaces, and a database of blocked users which prevents further attempts to access the services.

The most illustrative example of the "blacklisting" digital tool in this context is the Alibaba platform. It uses the most innovative proactive monitoring, detection and blocking measures, among which the "blacklisting" tool plays a sufficient role[45]. In case of repeated infringements, the platform permanently blocks the Bad Actor, whereby neutralizes the source of counterfeits, and reports to the enforcement bodies[46]. Using a similar approach, Youtube fights against online piracy and other copyright infringements, where the permanent blocking of the users is a final stage in the process[47].

Beyond the role of preventing online counterfeits and piracy, the "blacklisting" mechanism is intended to steer the commercial behaviour of market participants and to guarantee trustworthiness and confidence for the buyers which are currently at risk being attacked by malicious acts of Bad Actors.

---

[44] Katia Moskvitch, 'Russia's anti-internet piracy law faces backlash' (1 August 2013) *BBC News* <https://www.bbc.co.uk/news/technology-23510065> accessed 10 June 2019.

[45] Meeting with representatives of Alibaba Group at Alibaba's London Office (London, 30 January 2019).

[46] ibid

[47] See Google, *Community Guidelines strike basics,* <https://support.google.com/youtube/answer/2802032?hl=en> accessed 26 August 2019.

The tool should be backed by the rules and policies set by e-platforms for protection of IP. In consequence, a failure to obey them should lead to an access denial to an online marketplace and any of its services, that, in case of a dominant position of a particular e-platform, would make the excluded misbehaving participant "cyberspace-handicapped"[48]. Haucap and Heimeshoff also stress that such blockage would lead to the loss of investment into the trader's reputation and promotion on a particular marketplace and incur significant switching costs while changing platforms[49]. A consequence of switching to a smaller and less reputable platform will result in decreasing prices since the pricing mechanisms directly depends on the number of market participants on each platform[50]. In this fashion, the "blacklisting" tends to be an effective good behaviour stimulating tool.

III.2. DEFINITION AND MAIN CHARACTERISTICS

Most popular online dictionaries provide various definitions of "blacklists" which in general refer to the lists of people, organisations, countries who should be avoided considering by those who created these lists as unacceptable or untrustworthy[51]. Blacklisting terminology has been widely used in the politics, computing science, banking sphere, and other sectors. However, it is still obscure in the context of IP protection. In this respect, this Legal Opinion proposes to introduce the following autonomous definition of "blacklisting" which will emphasize the main characteristics of the tool:

"Blacklisting" is a universal technological tool used by state and law enforcement authorities, online platforms, service providers, or other online intermediaries, acting ex officio or upon the IP rightsholder's request, by which the persistent infringers are deprived of accessing online marketplaces or web-sites, where the repeated infringements have taken place, on a temporary or perpetual basis.

---

[48] Christina Hultmark, Christina Ramberg, and Christopher Kuner, *Internet marketplaces: the law of auctions and exchanges online* (Oxford University Press on Demand, 2002) 15.

[49] Justus Haucap and Ulrich Heimeshoff, *'Google, Facebook, Amazon, eBay: Is the Internet Driving Competition or Market Monopolization?'* (Discussion Paper No. 83, Düsseldorf Institute for Competition Economics (DICE) 2013) 11-12.

[50] ibid

[51] See, for example, Cambridge dictionary (online) <https://dictionary.cambridge.org/dictionary/english/blacklist> accessed 25 May 2019, or Oxford dictionary (online) <https://en.oxforddictionaries.com/definition/blacklist> accessed 25 May 2019.

As it follows, the first main beneficial feature of the "blacklisting" tool is its universality. This means that the tool can be used by everyone willing to prevent online infringements, including state and law enforcement authorities, online platforms, service providers, domain name registrars or other intermediaries. Secondly, the universality principle also refers to its use without territorial constraints, which could be a great advantage for international businesses and online community. Thirdly, the technological aspect of the tool will help to deal with massive amounts of data as well as velocity at which the data is disseminated, with lack of human intervention[52]. AI and Machine Learning, which enable working with big data at fastest speed, recognizing images and texts, identifying fraudulent actions and dealing with other complicated labour-consuming tasks[53], would sufficiently improve and enhance the tool, and help it to automatically detect and deny access to "blacklists" or "redlists" of traders. Fourthly, unlike other existing voluntary blocking measures[54], "blacklisting" does not require a court order or any other official authorisation – the infringer will be blocked based on the evidence of counterfeit sales, collected and assessed by the platform. Fifthly, upon a previously granted authority, the intermediaries may be free to operate without receiving the rightsholder's consent each time when the counterfeiting nature of products is detected, which will fasten the process of taking down the counterfeiting lists and blocking the source of their dissemination. Lastly, the tool can be easily integrated into the existing systems and business models and co-exist with other mechanisms and tools, along with bolstering the anticipated effects from their application. Compared to the existing methods, the "blacklisting" tool is aimed at tracking down the source of counterfeits, rather than singular infringements, that makes it a proactive step-forward measure.

Besides all of this, the tool may become of great help for the competent enforcement authorities in investigating online crimes. The complexity of the digital marketing and sale ecosystems makes it impossible to solely rely upon one solution, thus, a holistic approach is highly required[55]. In this vein, as Professor F. Mostert reasonably mentions "*digital tools used in combination with administrative measures, and based on due process, are possibly*

[52] However, human participation may be required for dealing with raised disputes or may be subject to obligations imposed by law.

[53] For further discussion about benefits of AI and ML for businesses – see Thomas H. Davenport, *The AI advantage: How to put the artificial intelligence revolution to work* (MIT Press 2018).

[54] For example, the Danish VCP (Code of Conduct) is aimed at establishing and facilitating of access blocking procedures for internet service providers and IP owners through court orders – see EUIPO Study (n 38) 22.

[55] Frederick Mostert and Jue WANG, 'The Application and Challenges of Blockchain in Intellectual Property Driven Businesses In China' (17 December 2018) Tsinghua China Law Review, Vol 11:13, 20.

the only way to counter the boom in both the volume and velocity of criminal activities online"[56].

It is clear that the system will require commitments from everyone: rightsholders should be proactive in proving information about their IPRs, monitoring online marketplace for the goods presented on them and reporting about alleged infringements; e-platforms should integrate a special technology to tackle repeated infringers; and governments should take necessary measures once the infringement is reported. In other words, the "blacklisting" serves as a connecting mechanism among all stakeholders.

III. 3. CLASSIFICATION OF LISTS

This Legal Opinion suggests a classification (ranking) of lists, which would function as a 'traffic light system'[57] indicating the level of credibility of each market player. A division into whitelisting and blacklisting[58] is already practically viable. Following this idea, it's proposed to make a more comprehensive graduation system to facilitate tackling infringements and provide more clarity and transparency of how the tool works.

This paper proposes to make four-step system which will comprise of "whitelist", "greylist", "blacklist" and "redlist". As it will be discussed further, while putting a seller into a particular list, a set of factors, such as traders' reputation, history of sales, commercial behaviour, and others, should be taken into account.

"Whitelist" is a list of trustful sellers who have a high level of credibility, based on the undisputable reputation, stable commercial businesses, and good trade behaviour. This list primarily includes rightsholders, as well as official distributors, licensees and other persons duly authorized by rightsholders to sell and promote genuine goods. This list may also comprise of those who are not directly authorized by rightsholders, but who have achieved the required level of trustworthiness, as mentioned above. For example, this may apply to sellers of genuine second hand goods seeking protection under a First Sale doctrine in the US or similar legal concepts in other countries. At the same time, re-sales of second hand goods

[56] Frederick Mostert (n 31).
[57] Weizmann Jacobs (n 1).
[58] Frederick Mostert (n 10) §116.

should be allowed unless they are unharmful to the rightsholder's reputation[59] and do not violate any of its rights.

The initial purpose of "whitelists" is to serve "as a reference point and checklist of authentic versus counterfeit"[60]. Apart from this, the "whitelists" may also refrain Bad Actors from increasing traffic to counterfeit listings for moving the products to the top of the search using fake reviews[61] and pre-paid advertisement, by giving a more comprehensive support and additional promotional benefits to the "whitelisters" subject to unfair competition rules (see further discussion in Part IV.1).

Amazon's Brand Registry Programme is one example of "whitelisting" that provides special additional tools to the rightsholders and trusted sellers to control the listing on the platform and efficiently remove potentially violating products.

"Greylist" (or "watchlist") serves as an interim stage for newcomers to the market, i.e. legal persons or individuals who have had no presence or previous trading history, or for those who have been involved in suspicious actions but have not caused sufficient damage to the market participants. The main aim of this type of lists is to scrutinise and control the "greylisters" actions.

The most well-known example of "greylists" (or "watchlists") which is currently used in the IP sector is the U.S. government's lists for countries which do not provide adequate and sufficient IP protection or enforcement of IPRs[62]. In the 2019 301 Special Report the "greylist" countries are those having "*the most onerous or egregious acts, policies, or practices and whose acts, policies, or practices have the greatest adverse impact (actual or potential) on relevant U.S. products"* [63]. Such countries are continuously scrutinized by the government and can be excluded from the lists, once they stop causing threat to the country's economy.

---

[59] For example, *Mary Kay v Weber* the court decided that sale of expired products "materially differ" from the original products, thus, this affect the plaintiff's name and reputation and constitutes the infringement see *Mary Kay Inc v Weber* 601 F.Supp.2d 839 (2009).

[60] Frederick Mostert (n 10) §120.

[61] Which? report, 'Amazon 'flooded by fake five-star reviews', *BBC News* (16 April 2019) <https://www.bbc.co.uk/news/business-47941181> accessed 28 May 2019.

[62] Executive Office of the President of the United States, *Special 301 Report 2019* (April 2019) 6.

[63] ibid 8.

Similar to the U.S. concept, intermediaries and rightsholders can transmit the general idea of "greylists" into e-commerce. Furthermore, online intermediaries may set specific time limits, sale targets, request documentation proving the originality of goods or content and apply any other additional measures to new sellers to confirm the legality of their businesses and their *bona fide* intentions.

"Blacklist", as being previously mentioned, is a list of blocked legal persons or individuals, who engage in, facilitate, or benefit from IP infringement or misappropriation of IPRs, or involved in related illegal activities. Once being included into a "blacklist", a person will be deprived of any access to trading on the platform or web-site where the infringing goods have been sold or illegal content has been uploaded. The ban can be temporary or permanently, depending on the circumstances of the case and subsequent actions of the infringer.

One of the proposed criteria for "blacklisting" of the repeated infringers is to use a three-strike, or a graduated response, policy. This policy is acknowledged to be both an easy-to-apply and effective one. Moreover, some countries[64] have already passed such policies into their national laws to tackle copyright infringement, and more others are considering this approach[65]. E-platforms, such as Alibaba and Youtube also use a three-strike policy which, if happened, will lead to account permanent ban.

Specifically, a "three-strike policy" comprises of the following stages: an individual alleged in infringing IPRs is alerted as a first step, with a right to provide evidence of acting in a good faith; then he is warned about the consequences of continuing the illegal action as a second step, and he is "blacklisted", with immediate access block, as a third and final step.

"Redlist" (or "red-flagging list") is reserved for criminals who have been recognized as such by enforcement authorities. Unlike "blacklists" containing alleged infringers, "redlists" include those against which the court or police have taken legal actions. Such lists should be open to the public and serve as a warning notice to customers willing to buy products from untrusted sources. At the same time, the idea of public communication of counterfeit products

[64] For example, China, New Zealand, France, South Korea, Taiwan, etc.

[65] Jordi McKenzie, '*Graduated response policies to digital piracy: Do they increase box office revenues of movies? Information Economics and Policy'* (Volume 38 Elsevier 2017) 2-3.

is not supported by some industries. For example, WHO concerns that alarming patients and the public about counterfeiting medicine would result in undermining confidence in medical services[66]. On the other hand, dissemination of knowledge about counterfeits and piracy as well as "redlist" of criminals would raise awareness about the problem and its consequences among public as well as protect consumers from buying products from illegal sources.

Switching from one list to another should fully rely on a commercial behaviour pattern of each trader. The question on how this behaviour should be assessed remains open for consideration. Alibaba, for example, uses a points-based penalty system, whereby in case of IPR infringement the trader is penalized by search ranking reduction, listings blockage or limitation to advertising tools[67]. As a suggestion, combining this system with a positive rewarding points-based system, based on good behaviour history record, identity verification results, user assessment and other set criteria, may help to assess the commercial behaviour and, subsequently, move the user to corresponding lists.

III. 4. IMPLEMENTATION STAGES

This part will describe a three-step integration process of "blacklisting" digital tool, which could be used as a guideline for everyone willing to implement the tool.

Stage One. Introduction and increase of awareness of the "blacklisting" tool

The primary objective of this stage is to introduce the "blacklisting" digital tool to a greater number of market players and state authorities as an alternative or additional method to combat online counterfeits and pirated goods.

In this regard, Alibaba's and Youtube's progress and success may serve as a convincing example for other online platforms. So can be the PIPCU's and Chinese government's experience - for state authorities.

---

[66] WHO,*WHO Global Surveillance and Monitoring System for substandard and falsified medical products* (Geneva, 2017) 57.

[67] Alibaba Group, *Alibaba Intellectual Property Protection Handbook*, <https://ipp.alibabagroup.com/infoContent.htm?skyWindowUrl=notice/handbook-en> assessed 4 August 2019, 7.

Dissemination of this knowledge can be made through educational processes and awareness activities in the form of seminars, workshops, etc., as well as the benefits of the tool can be discussed at international summits and conferences or advertised via anti-counterfeiting campaigns.

Stage Two. Collaborative efforts

It has become clear that significant success in countering the proliferation of counterfeit and pirated goods can be achieved only through cooperative efforts of all users, rightsholders, intermediaries and governments. Further, INTA's "Best Practices for Addressing the Sale of Counterfeits on the Internet" emphasises the need to share as much data as possible among search engines, trading platforms, payment service providers, social media sites, registrars and registries[68]. Nowadays sharing of information about the alleged illicit actions is also supported and encouraged by the legislature. For example, the E-Commerce Directive[69] allows member states to establish obligations for information society service providers to inform the competent authorities of alleged illegal activities and provide supporting information to detect infringers (Art. 15 (2)).

A big step in consolidating forces of the rightsholders and enforcers has been made recently by EUIPO, through the European Observatory on Infringements of IP Rights, by introducing an IP Enforcement Portal, which serves as a uniform single platform aimed at facilitation of the IP enforcement procedures as well as a secure communication tool between the market players, enforcers and the EU Commission with its delegates.

This Legal Opinion proposes to further upgrade the Portal or create a similar platform by including the "blacklisting" database of counterfeiters to be shared among the participants, by extending the territory to other countries and by providing the access for other market participants, including, for instance, e-marketplaces and online payment systems, in order to avoid duplication of efforts. Ideally, this should become a global platform which is designed to cover the whole chain of users, intermediaries and enforcers. Hence, this would help to

[68] International Trademark Association, *Addressing the Sale of Counterfeits on the Internet (2017)* <https://www.inta.org/Advocacy/Documents/2018/Addressing_the_Sale_of_Counterfeits_on_the_Internet_021518.pdf> accessed 04 August 2019, 4.

[69] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-commerce Directive).

facilitate the detection of bad actors and further prevention of their illegal activities, insofar as it is permitted by current data protection legislation (see further discussion in Part IV.3).

A new model of collaboration between all stakeholders underlies the universality principle of the "blacklisting" digital tool. In other words, collective forces and mutual information exchange and sharing form a basis for its effective use and achievement of the anticipating results. The use of "blacklisting" tool and establishment of global "blacklisting" portal (database) are key points for the proper functioning of the mechanism in general.

Stage Three. Global guidance of "blacklisting" tool

Once being successfully implemented, the "blacklisting" universal tool would require a uniform and harmonised regulation to enhance its efficiency as well as to diminish uncertainty and ambiguity in its use by various market players in different jurisdictions. It has become obvious that national and regional laws won't be able to cope with this task and will be counter-productive since they can deal with only local fragments of the Internet[70]; worse than this could be discrepancies and gaps the local regulation may cause. In other words, effective regulation of online marketplaces dealing with cross-border issues cannot be reached by national rules. Beyond that, a single national state can hardly have authority over the cyberspace due to their territorially limited powers[71].

Although most market players have been used to national regulation, it is clear that the only reasonable solution can be reached by self-regulatory means, providing a harmonised and coherent approach to regulation of the universal "blacklisting" tool. This can be made in the form of a voluntary agreement, following the example of a Memorandum of Understanding, which is facilitated by the European Commission to prevent offers of counterfeit goods from appearing in online marketplaces[72] or a uniform code of practice. This idea has already been accepted by major Internet companies, such as Google, Twitter and Facebook who have agreed to collaborate with the UK Government to establish the social media code of practice and transparency reporting[73]. Further, the market players can establish "virtual communities" to enforce the created rules.[74] Or, as an alternative, the UK government has proposed to

[70] Frederick Mostert (n 31)
[71] Christina Hultmark *et al.* (n 45) 13
[72] European Commission, *Memorandum of Understanding* (Brussels, 21 June 2016).
[73] HM Government, *Government Response to the Internet Safety Strategy* (Green Paper, May 2018) 9.
[74] Debora Spar and Jeffrey J. Bussgang, 'Ruling the Net' (1996) *Harvard Business Review*, 125.

appoint an independent regulator whose main duties would be producing and enforcing codes of practice, preparing transparency reports, and educating the online community[75].

The codes of practice could be also underpinned by various sanctions and fines, to be levied on e-platforms which do not comply with the proposed regulations, in order to increase their responsibility.

IV. BLACKLISTING AND CURRENT LEGISLATION

The process of integrating the "blacklisting" tool may face two major obstacles: technological feasibility and compliance with existing laws. And while the technological obstacle solely depends on the investment opportunities and facilities of a particular market player, the norm-setting framework needs deep analytical analysis and subsequent changes.

As noted in Part 1 of the Legal Opinion, the legislators fall far short of technological possibilities and corresponding counterfeiting tendencies. Hence, it is highly recommended that the national states should be less regulatory towards online marketplaces and digital tools, considering their lack of ability to effectively and promptly react to the continuous changes. And, on the opposite, they should facilitate their self-regulation and applicability of digital tools to monitor and control the process of original products sales and ban of counterfeit dissemination.

However, this does not mean that the laws should totally ignore regulation of marketplaces or control the use of technological tools. In particular, preventing abuse in using digital tools, including the "blacklisting" tool, should remain a primary purpose of the legislation. Therefore, maintaining a fair balance between the use of an access denial mechanism or other preventive tools and the fundamental rights to fair competition, free speech and expression, and personal data protection should take place at each stage of implementation of the "blacklisting" mechanism.

Having realised the necessity of finding this balance, the EU Commission has recently implemented a new Regulation[76] for promoting fairness and transparency in e-trading on

[75] HM Government (n 32) 8-9.

digital platforms for businesses established in the EU. In the context of "blacklisting", Recitals 22-24 and Art. 4, as long with some of their supporting provisions, are of the main interest for discussion. The provisions allow the platforms to restrict, suspend or terminate its services including by delisting of goods or services or removing search results, however, with an imposed obligation to provide the users with a statement of reasons for such decision within at least thirty days before the termination (Recital 22 and Art. 4 (1)). The business users are entitled to a number of other safeguards, such as transparency and easy access of terms and conditions, providing *inter alia* the grounds for termination of services (Art. 3 (1)(c)), the internal complaint-handling system for dealing with requests and complaints of business users (Art. 11), transparency of personal data use (Recitals 33-35 and Art. 9), and prompt reinstatement of business user's status (Art. 4 (3)) with effective redress possibilities (Art 1).

Despite these generous safeguards for business users, the EU Commission successfully stroke a fair balance, by introducing a set of limitations to these safeguards in case of the whole termination of services due to repeated infringements of terms and conditions, i.e. "blacklisting" (Art. 4 (4)(c)). So, in particular, while "blacklisting" the user, the platform is not obliged to follow the requirements of thirty-day notice and to provide a statement of reasons for termination of services. In this fashion, the legislature provides more stringent measures towards repeated infringements.

Notwithstanding the above big step in a balanced regulation of e-platforms' activities in the EU, from a global view, there are still some legal uncertainties and controversies, whilst applying the "blacklisting" tool, which will be further discussed in this part of the Legal Opinion.

IV. 1. Blacklisting and Competition Law

[76] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services PE/56/2019/REV/1 (**"Platform-to-Business Regulation"**).

Already in 1914 in debates upon the Federal Trade Commission Bill[77] Senator Robinson, while proposing the notion of unfair competition[78], referred to the economist W. S. Stevenson of Columbia University, who named "whitelists" and "blacklists" as one of eleven forms of unfair competition from an economic standpoint[79]. Although these notions as such were not introduced in the new law and can be hardly found in existing laws, unfair discrimination and groundless access denial or limitation to online markets as such may serve as a violation of the basic principles of free competition.

In the given context, nowadays, many questions have raised with the emergence and development of digital markets as to whether existing competition law rules can successfully regulate the challenges created by the technological developments[80]. Main concerns relate to defining digital markets and the dominance position under traditional rules due to their specific business models based on free services, easy switch and the ownership of data as a key factor in market influence[81]. Notwithstanding these difficulties, the leading e-platforms, including *Google, Facebook, eBay, Amazon, etc.,* are subject to constant antitrust scrutiny[82] and, as to date, with increasing frequency become defendants in antitrust cases[83].

Therefore, e-platforms are in the centre of attention of anticompetition authorities as well as their actions aimed at prevention of certain business users to their services via the "blacklisting" digital mechanism. Hence, the digital tool and the proposed classified set of lists may be at risk of contradicting with the existing competition and antitrust rules.

Therefore, in order to mitigate such risks, it is advised to consider the basic safeguards, proposed by the Platform-to-Business Regulation within the EU territory or by academic community for situations beyond the scope of the said regulation, such as transparency of policies, proportionality of use, fines for misuse, the possibility to contest decision on

---

77 The Federal Trade Commission Act (Public, No. 2o3, 63d Congress H. R. 15613, approved 6 September 1914).

78 Senator Robinson, Congressional Record, (vol. 51, 1914), 12248.

79 William S. Stevens, 'Unfair Competition' (1914), *Political Science Quarterly*, vol. 29 (2), 282-306, doi:10.2307/2141775, 284.

80 Richard Hourihan and Joanne Finn, 'Google and the six billion dollar fine(s): We have the technology, but do we have to rebuild the competition rules?' (*Wolters Kluwer Law Blog* 18 April 2019) <http://competitionlawblog.kluwercompetitionlaw.com/2019/04/18/google-and-the-six-billion-dollar-fines-we-have-the-technology-but-do-we-have-to-rebuild-the-competition-rules/> accessed 18 August 2019.

81 ibid

82 For a discussion, see Justus Haucap and Ulrich Heimeshoff (n 46) 8-15.

83 For example, *Google Search (Shopping)* (2010), *Google AdSense* (2016), etc.

"blacklisting" and others[84]. In addition to this, E-platforms should base their decisions solely on stringent evidence of IP infringement, and immediately rehabilitate the users, once the decision is challenged.

Regarding the grading system, which includes "whitelists" that give a certain market player additional advantages on e-marketplaces, e-platforms must ensure that they are not subject to abuse. In order to provide compliance of "whitelists" with the existing laws, Professor F. Mostert proposes to limit their function to "indicative measures" for customers[85]. Also, moving beyond the sole indicative function, the solution could be found in implementing the online rating point-based system, as proposed earlier, which promotes fair competition depending on the positive behaviour of each market player. The above ideas can be supported by the requirement of ranking parameters and mechanisms transparency, proposed by the Platform-to-Business Regulation, which obliges the platform to describe in their terms and conditions the main algorithms determining rankings of results and lists of individual goods and services[86].

Though the EU legislature has made a successful attempt in implementing the rules to suppress unfair practices of dominant digital platforms, at a global scale, the interrelation between the competition rules and new technological measures, including "blacklisting", lacks regulation and, thus, requires future law reforms.

IV. 2. Blacklisting and Freedom of Speech Law

Constitutions of various jurisdictions and human rights international treaties recognise the right to freedom of expression and speech and require from national governments and their authorities to protect these rights. In the IP context, Advocate General Jääskinen in his opinion in *L'Oreal v eBay case* has explicitly stated that the listings of goods uploaded by users are "*communications protected by the fundamental rights of freedom of expression and*

[84] Frederick Mostert (n 10)§120.
[85] Frederick Mostert, 'Digital Tools of Intellectual Property Enforcement – their intended and unintended norm-setting consequences', chapter in *Research Handbook on IP and Digital Technologies*, edited by Tanya Aplin (in press 2019).
[86] Recitals 24-27 and Art. 5

information provided by Article 11 of [the] Charter of Fundamental Rights of the EU and Article 10 of the European Convention on Human Rights"[87].

In this vein, new technologies, including take-down notices or "blacklisting", preventing dissemination of information about the goods and services, deleting the listings or banning the sources of such information may infringe these rights. As a result, the consuming public would receive less diverse information on goods and services in the digital environment[88].

For example, once "blacklisted", a person will be deprived of any possibility to further publish information about the goods for sale, or content they have uploaded, which may breach the laws protecting freedom of expression. At the same time, the Bad Actors engaged in counterfeiting activities may use a "free speech" to hide behind its tenet[89] and may avail themselves of all services provided by e-platforms. A key issue arising with this regard is the balancing, on the one hand, of the freedom of expression, which lies in the public interest, with the private interest of trading businesses, on the other hand.

Alan Howard, Professor of Law, indicates the primary purposes of speech as helping to make for its "listeners" an informed decision[90]. In the context of e-commerce, this means that the consumers should receive accurate information about the products they are willing to purchase or copyrighted work they are consuming. However, in case of counterfeits and piracy, the consumers are deceived by false and misleading statements about the 'originality' of goods or published materials, converting the information presented to a deceptive one, which in its turn should not enjoy protection.

For example, in the US infringing uses of trademarks for selling counterfeit goods are not protected under the First Amendment if they constitute misleading commercial expression[91]. This is also supported by national courts which reject free-speech-based arguments in case of deceptive speech[92]. Therefore, the main task of the court is to verify if defendant's use is

---

87 Advocate General N. Jääskinen, Opinion of 9 December 2010, C-324/09 *L'Oreal v eBay* [2011], para 49

88 Martin Senftleben, 'An Uneasy Case for Notice and Takedown: Context-Specific Trademark Rights' (16 March 2012) <https://ssrn.com/abstract=2025075> accessed 12 August 2019.

89 Frederick Mostert, 'The global digital enforcement of intellectual property' (September 2018), WIPO Magazine, <https://www.wipo.int/wipo_magazine/en/2018/si/article_0005.html> accessed 15 August 2019.

90 Alan Howard, 'The Constitutionality of Deceptive Speech Regulations: Replacing the Commercial Speech Doctrine with a Tort-Based Relational Framework', (1991), 41*Case West. Res. L. Rev.* 1093, 1109.

91 Lisa P Ramsey, 'A Free Speech Right to Trademark Protection' (106 Trademark Reporter 2016) 871.

92 Frederick Mostert (n 10) §45.

deceptive[93] and to weigh and balance between the competing legitimate interests of all market players[94].

Despite the court findings, in order to avoid the breach of the said fundamental rights by over-removal of legal listings and content or over-blocking of users via the "blacklisting" mechanism, e-platforms should foresee adequate safeguards similar to those proposed earlier for balancing the freedom of competition and the "blacklisting" use.

IV. 3. Blacklisting and Data Protection Law

The protection of personal data and privacy is one more fundamental right proclaimed by international conventions and national laws, and in the digital environment, it becomes more vulnerable due to the high risk of leakage. This forces the national states to strengthen protection and make the punishment for its infringement more rigorous. However, the adverse effect of too rigid rules has led to the distraction of the investigation of cybercrimes[95]. For example, in order to comply with newly implemented EU Regulation on Data Protection[96], the Internet Corporation for Assigned Names and Numbers (**"ICANN"**) was forced to change its policy and to limit access to domain registration data (Whois), containing personal data, which had been previously located in the public domain and could be easily used to detect the alleged infringer. This severely impacted the possibility to tackle the online infringements and prevent harm to victims of counterfeiting[97]. Overprotection of data, therefore, has created adverse consequences for investigating cyber-crimes and enforcing IP rights, that pose serious threats to public safety.

---

93 Leonardo Machado Pontes, 'Trademark and Freedom of Speech: A Comparison between the U.S. and the EU System in The Awakening of Johan Deckmyn V. Helena Vandersteen' *WIPO Magazine* (18 May 2015) WIPO/IPL/GE/15/T3 <https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=303857> accessible 15 August 2019.

94 Frederick Mostert (n 85)

95 Dave Piscitello, 'EU GDPR Compliance Implementation Creates Adverse Consequences for Cyber Investigations' (27 May 2019) <https://apwg.org/830-2/> accessed 10 August 2019.

96 Regulation (EU) 2016/679 Of The European Parliament And Of The Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (27 April 2016) (**"GDPR"**).

97 Maysa Razavi and Lori S Schulman, 'Counterfeiting and data privacy: achieving the right balance in consumer protection' (13 May 2019) *World Trademark Review* <https://www.worldtrademarkreview.com/anti-counterfeiting/counterfeiting-and-data-privacy-achieving-right-balance-consumer-protection> accessed 9 August 2019.

At the same time, public safety must be treated as equally important as the protection of personal data – and the rules regulating the personal data should not prevent protection of health and lives of people who may become victims to counterfeiting products. As is reasonably mentioned by the UK government "ensuring people's safety online is a fundamental element of this thriving ecosystem"[98].

As is discussed above, the EU GDPR, having considerable influence around the world, has sufficiently changed the global landscape of privacy and data protection. As a result, one of the biggest tensions have appeared between GDPR and big data[99] and innovative technological tools based on it. Applying this view to the "blacklisting" tool, it's fair to state that too rigid data protection rules can also challenge its free implementation and use on the digital market, since at the heart of the "blacklisting" lies massive data collection, storage and use that is subject to obligations under data protection laws. Moreover, the shared information about the "blacklisted" infringers could also contradict with current laws.

Severe sanctions and outrageous fines[100] for violation of the GDPR provisions may also become a serious obstacle for promoting of the "blacklisting" tool in the digital community. This Legal Opinion will try to further clarify whether the "blacklisting", consisting of a blocking tool and a database of blocked users, may comply with the objectives of the GDPR and its lawful basis for processing personal data.

In a broad term, the GDPR provisions prescribe obligation to comply with its main principles, such as lawfulness, fairness and transparency (Recital 39, Art. 5(1)(a) and Art. 6), limitation purpose (Art. 5(1)(b)), data minimisation (Art. 5(1)(c)), data accuracy (Art. 5(1)(d)), storage limitation (Art. 5(1)(e)), data security, including integrity and confidentiality

---

[98] HM Government (n 73).

[99] Tal Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (8 August 2017) *Seton Hall Law Review*, Vol. 47, No. 4(2), 2017 <https://ssrn.com/abstract=3022646> accessed 9 August 2019.

[100] The largest fine to date in the amount of £183.39m under the EU's GDPR has been levied on British Airways which has compromised its employee's personal data as a result of a cyber incident - Information Commissioner's Office, *'Intention to fine British Airways £183.39m under GDPR for a data breach'* (Statement, 08 July 2019) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-ico-announces-intention-to-fine-british-airways/> accessed 5 August 2019.

(Art. 5(1)(f)) and accountability (Art. 5(2))[101]. This imposes a severe burden on the processor of data and makes the use of the tool unrealistic.

On the other hand, as GDPR recitals explicitly state, privacy is not an absolute right and must be balanced with other interests and fundamental rights (for ex., Recital 4). First, GDPR provides a general exception for safeguarding the prevention, investigation, detection or prosecution of criminal offences, including threats to public security, or the execution of criminal penalties, allowing the member state to restrict the scope of the obligations and rights regulated by the law (Art 23.1 (d)). Second, the underlying processes of making the automated decision based on search, storage and use of data with the "blacklisting" tool are generally prohibited by Art. 22(1), unless they fall within the scope of exceptions provided by Recital 71 and Art. 22 (2). Professor Tal Zarsky also states that the violation can be escaped by inserting minimal human interaction[102]. Thus, analysis so far suggests that for e-platform in order to comply with the following provisions of GDPR, there are some safeguards that should be always included where there is a legal basis assisting the exchange of personal data. It's suggested for e-platforms to draft carefully their contracts and data protection policies, bearing in mind these exceptions and the explicit consent to the use of data while making the decision which may affect the users. In addition, e-platforms should implement easily accessible mechanisms for challenging such decision and request human review[103].

Considering the above, the "blacklisting" tool used for its initial purpose of banning the counterfeiters and pirates by platforms, could comply with the GDPR rules, though the situation is still uncertain with a shared database of "blacklisted" and "redlisted" infringers. As to date, once and if the information becomes public, this echoes the ICANN's situation with regard to limits on sharing information about domain name holder. Hence, the implementation of GDPR has left the digital industry demanding mitigation of privacy and requesting the governments to recognise the importance of information-sharing functions that exist between law enforcement and the private sector.

[101] For more information about the principles see Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights, *Handbook on European data protection law* (16 May 2019) 115-137.
[102] Tal Zarsky (n 99).
[103] Frederick Mostert (n 84).

V. CONCLUSION

Since 1994 when the first online transaction was made[104], e-commerce has evolved significantly and re-shaped business practices and consumer behaviour. It has given unlimited opportunities to the rightsholders to expand their trade globally, avoiding time and geographical limits. At the same time, it has also provided a great expansion of counterfeiting industry, which uses the technological benefits of e-commerce in a more sophisticated way, that gives them an undeniable advantage to win in the battle over the rightsholders, intermediaries and law enforcers. As a result, a search for innovative effective tools to combat online infringers has become a high-priority matter for governments and businesses around the world.

In this fashion, "blacklisting" is viewed as a promising mechanism in the pursuit by government and industry for the prevention and deterrence of counterfeit and piracy growth in the digital environment. In a broader sense, the tool can also monitor, rate, and steer the conduct of market participants, and contribute to building up a new culture of e-commerce in the future.

Moreover, the tool would organically fit in the existing anti-counterfeiting programmes, and, more than that, may co-exist with other digital tools and bolster their effect accordingly. The only main challenges in implementing the "blacklisting" tool which the stakeholders may face are technological feasibility, which requires sufficient expenses to employ and support a big-data AI technology, and current legislation which prevents the free use of the "blacklisting" tool.

Considering this issue from a legal standpoint, it is advised to support the development of the "blacklisting" mechanism by creating a more friendly legal environment for the use and implementation of technological measures, helping to combat illegal actions in the online community. In this regard, the role of legislators is crucial for stimulating self-regulation of

[104] Peter H. Lewis, 'Attention Shoppers: Internet Is Open' (August 12, 1994), *NY Times.* Digital version is available at <https://www.nytimes.com/1994/08/12/business/attention-shoppers-internet-is-open.html> accessed 18 August 2019.

e-platforms and development of new technology aimed at the protection of legal e-commerce, whilst keeping a fair balance between fundamental rights and the newly developing rules.

To sum up, the main purpose of this Legal Opinion is to expose knowledge about the "blacklisting" tool with a theoretical proposal of its classification and implementation stages. Beyond raising awareness of the "blacklisting" digital tool, the paper also urges to take an active role in its development which is required from all stakeholders, by invoking the tool into online protecting systems and building up the "blacklisting" database. This all should be underpinned by the creation and further obeyance of code of practice, which will provide clear guidance and global standards for applying the "blacklisting" tool.

BIBLIOGRAPHY

LEGISLATION:

The Federal Law No. 187-FZ of July 2, 2013 On Amending Certain Legislative Acts of The Russian Federation on Issues of Protecting Intellectual Rights in Information Telecommunication Networks

The Federal Trade Commission Act (Public, No. 2o3, 63d Congress H. R. 15613, approved 6 September 1914)

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-commerce Directive)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR")

Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services PE/56/2019/REV/1

CASES:

Mary Kay Inc v Weber , 601 F.Supp.2d 839 (2009)

Google AdSense, Case 40411 (2016)

Google Search (Shopping), Case AT.39740 (2017)

L'Oréal SA v eBay International AG, Case C-324/09 (2011)

OFFICIAL REPORTS AND PAPERS:

European Commission, 'Report on the EU customs enforcement of intellectual property rights. Results at the EU border' (2017)

European Commission, Memorandum of Understanding (Brussels, 21 June 2016)

Europol, 'SOCTA: EU Serious and Organised Crime Threat Assessment, Publications Office of the European Union', (Luxembourg, 2017)

EUROPOL/EUIPO, '2017 Situation Report on Counterfeiting and Piracy in the European Union' (2017) <https://www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union> accessed 4 June 2019

Executive Office of the President of the United States, Special 301 Report 2019 (April 2019)
HM Government, 'Government Response to the Internet Safety Strategy' (Green Paper, May 2018)

HM Government, 'Online Harms' (White Paper, April 2019)

Hoeren T, Westkamp G, Vidal M, Rodriguez Ballano S, Iun P, De Lluc Compte A, Pascual J, Sánchez Guarido A and Torres J, 'Study on Voluntary Collaboration Practices in Addressing Online Infringements of Trade Mark Rights, Design Rights, Copyright and Rights Related to Copyright' (September 2016), *EUIPO* <https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Research%20and%20studies/study_voluntary_collaboration_practices_en.pdf> accessed 1 August 2019

OECD/EUIPO, '*Misuse of Small Parcels for Trade in Counterfeit Goods: Facts and Trends'*, (OECD Publishing, Paris, 2018)

OECD/EUIPO, 'Trends in Trade in Counterfeit and Pirated Goods, Illicit Trade', (2019 OECD/EUIPO Report, Paris, 2019)

U.S. Customs and Border Protection Office of Trade, 'Intellectual Property Rights, Fiscal year 2017 Seizure Statistics (2017)

<https://www.cbp.gov/sites/default/files/assets/documents/2019-Apr/FY%202017%20Seizure%20Stats%20Booklet%20-%20508%20Compliant.pdf> accessed 13 July 2019

US Chamber of Commerce, 'Measuring the magnitude of global counterfeiting: creation of a contemporary global measure of physical counterfeiting' (Washington DC, 2016), <https://www.uschamber.com/sites/default/files/documents/files/measuringthemagnitudeofglobalcounterfeiting.pdf> accessed 16 June 2019

BOOKS:

Davenport T H, The AI advantage: How to put the artificial intelligence revolution to work (MIT Press 2018)

Global Brand Counterfeiting Report, 2018 (R Strategic Global, December 2017)

Hultmark C, Ramberg C, and Kuner C, Internet marketplaces: the law of auctions and exchanges online (Oxford University Press on Demand, 2002)

McCarthy Th J, Trademarks and Unfair Competition (4th ed., 2014)

Mostert F, 'Digital Tools of Intellectual Property Enforcement – their intended and unintended norm-setting consequences', chapter in Research Handbook on IP and Digital Technologies, edited by Tanya Aplin (in press 2019)

JOURNAL ARTICLES:

Grimes S, Cheng G and Zhao Y, 'China Says It Will Blacklist and Sideline Repeat Intellectual Property Right Violators' (10 December 2018) Lexology <https://www.lexology.com/library/detail.aspx?g=a25c6c93-4624-4925-b3bf-c6bb55478d2d> accessed 31 May 2019

Haucap J and Heimeshoff U, 'Google, Facebook, Amazon, eBay: Is the Internet Driving Competition or Market Monopolization?' (Discussion Paper No. 83, Düsseldorf Institute for Competition Economics (DICE) 2013)

Howard A, 'The Constitutionality of Deceptive Speech Regulations: Replacing the Commercial Speech Doctrine with a Tort-Based Relational Framework', (1991), 41Case Western Reserve Law Review 1093, 1109

McKenzie J, 'Graduated response policies to digital piracy: Do they increase box office revenues of movies? Information Economics and Policy' (Volume 38 Elsevier 2017)

Mostert F, 'Study On Approaches To Online Trademark Infringements' (1 September 2017) WIPO/ACE/12/9 REV. 2

Mostert F and WANG J, 'The Application and Challenges of Blockchain in Intellectual Property Driven Businesses In China' (17 December 2018) Tsinghua China Law Review, Vol 11:13

Mostert F, 'Study on IP Enforcement Measures, Especially Anti-Piracy Measures in The Digital Environment' (3 July 2019) WIPO/ACE/14/7

Mostert F, 'The global digital enforcement of intellectual property' (September 2018), WIPO Magazine, <https://www.wipo.int/wipo_magazine/en/2018/si/article_0005.html> accessed 15 August 2019

Pontes L M, 'Trademark and Freedom of Speech: A Comparison between the U.S. and the EU System in The Awakening of Johan Deckmyn V. Helena Vandersteen' WIPO Magazine (18 May 2015) WIPO/IPL/GE/15/T3 <https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=303857> accessible 15 August 2019

Senftleben M, 'An Uneasy Case for Notice and Takedown: Context-Specific Trademark Rights' (16 March 2012) <https://ssrn.com/abstract=2025075> accessed 12 August 2019.

Spar D and Bussgang J J, 'Ruling the Net' (1996) *Harvard Business Review*

William S. Stevens, ‘Unfair Competition’ (1914), *Political Science Quarterly*, vol. 29 (2), 282-306, doi:10.2307/2141775

Zarsky T, ‘Incompatible: The GDPR in the Age of Big Data’ (8 August 2017) Seton Hall Law Review, Vol. 47, No. 4(2), 2017 <https://ssrn.com/abstract=3022646> accessed 9 August 2019.

NEWSPAPER ARTICLES:

Krouse S and O'Keefe K, ‘Senators Introduce Bill Restricting Huawei From Buying, Selling U.S. Patents, the Wall Street Journal’ (The Wall Street Journal, 18 July 2019) <https://www.wsj.com/articles/senators-to-introduce-bill-restricting-huawei-from-buying-selling-u-s-patents-11563463179> accessed 21 July 2019

Lewis P H, ‘Attention Shoppers: Internet Is Open’ (August 12, 1994), NY Times. Digital version is available at <https://www.nytimes.com/1994/08/12/business/attention-shoppers-internet-is-open.html> accessed 18 August 2019

Moskvitch K, ‘Russia's anti-internet piracy law faces backlash’ (1 August 2013) BBC News <https://www.bbc.co.uk/news/technology-23510065> accessed 10 June 2019

Mostert F, ‘The Internet: Regulators Struggle To Balance Freedom With Risk’ (Financial Times, 9 July 2019) https://www.ft.com/content/e49c39e6-967d-11e9-8cfb-30c211dcd229 accessed 11 July 2019

Smialek J, Tankersley J and Ewing J, ‘Global Economic Growth Is Already Slowing. The U.S. Trade War Is Making It Worse’, *N.Y. Times*, (New York, 18 June 2018) <https://www.nytimes.com/2019/06/18/business/economy/global-economy-trade-war.html> accessed 8 July 2019

Which? report, ‘Amazon 'flooded by fake five-star reviews', BBC News (16 April 2019) <https://www.bbc.co.uk/news/business-47941181> accessed 28 May 2019

DICTIONARIES:

Cambridge dictionary (online)
<https://dictionary.cambridge.org/dictionary/english/blacklist> accessed 25 May 2019

Oxford dictionary (online)
<https://en.oxforddictionaries.com/definition/blacklist> accessed 25 May 2019

OTHERS:

Alibaba Group, *Alibaba Intellectual Property Protection Handbook*, <https://ipp.alibabagroup.com/infoContent.htm?skyWindowUrl=notice/handbook-en> assessed 4 August 2019

Alibaba Group, Meeting at Alibaba's London Office (London, 30 January 2019)

Blackburn D, Eisenach J A and Harrison Jr D, 'Impacts of Digital Video Piracy on the U.S. Economy' (June 2019) < https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf> accessed 26 August 2019

Council of Europe, European Court of Human Rights , European Data Protection Supervisor, European Union Agency for Fundamental Rights, 'Handbook on European data protection law' (16 May 2019)

Doug Palmer, Melanie Lee, 'Special report: Faked in China: Inside the pirates' web' (26 October 2010) *Reuters* <https://www.reuters.com/article/us-china-counterfeit-idUSTRE69P1AR20101026> accessed 11 July 2019

Frontier Economics, *'The Economic Impacts of Counterfeiting and Piracy'* (Report prepared for BASCAP and INTA, February 2017)

Google, *Community Guidelines strike basics,* <https://support.google.com/youtube/answer/2802032?hl=en> accessed 26 August 2019

Hourihan J and Finn J, 'Google and the six billion dollar fine(s): We have the technology, but do we have to rebuild the competition rules?' (*Wolters Kluwer Law Blog* 18 April 2019) <http://competitionlawblog.kluwercompetitionlaw.com/2019/04/18/google-and-the-six-billion-dollar-fines-we-have-the-technology-but-do-we-have-to-rebuild-the-competition-rules/> accessed 18 August 2019

Information Commissioner's Office, *'Intention to fine British Airways £183.39m under GDPR for a data breach'* (Statement, 08 July 2019) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-ico-announces-intention-to-fine-british-airways/> accessed 5 August 2019

International Trademark Association, *Addressing the Sale of Counterfeits on the Internet (2017)* <https://www.inta.org/Advocacy/Documents/2018/Addressing_the_Sale_of_Counterfeits_on_the_Internet_021518.pdf> accessed 04 August 2019

Jacobs W, Interview (King's College London, 14 November 2018)

Joelle Bergeron, '*Working document on three-dimensional printing, a challenge in the fields of intellectual property rights and civil liability'*, Committee on Legal Affairs of European Parliament (23 November 2017)

Julia Dickenson, Jason Raeburn Katrina Thomson, 'Procedures and strategies for anti-counterfeiting: United Kingdom' (14 May 2019) *World Trademark Review* <https://www.worldtrademarkreview.com/anti-counterfeiting/procedures-and-strategies-anti-counterfeiting-united-kingdom-1> accessed 14 July 2019

Morrison & Foerster, 'Preparing for the Increased Globalization of IP Litigation' (Study, 7 August 2019) <https://mofotech.mofo.com/topics/preparing-increased-globalization-ip-litigation.html> accessed 10 August 2019

'PIPCU disrupts £719 million worth of IP crime' (Press Release, 21 January 2019) <http://news.cityoflondon.police.uk/r/1184/pipcu_disrupts__719_million_worth_of_ip_crime> accessed 4 June 2019

Piscitello D, ‘EU GDPR Compliance Implementation Creates Adverse Consequences for Cyber Investigations’ (27 May 2019) <https://apwg.org/830-2/> accessed 10 August 2019

Ramsey L P, 'A Free Speech Right to Trademark Protection' (106 Trademark Reporter 2016)

Razavi M and Schulman L S, ‘Counterfeiting and data privacy: achieving the right balance in consumer protection’ (13 May 2019) *World Trademark Review* <https://www.worldtrademarkreview.com/anti-counterfeiting/counterfeiting-and-data-privacy-achieving-right-balance-consumer-protection> accessed 9 August 2019

Senator Robinson, Congressional Record, (vol. 51, 1914), 12248. Digital version available at <https://www.govinfo.gov/app/details/GPO-CRECB-1914-pt18-v51/GPO-CRECB-1914-pt18-v51-3/context>

Stroppa A, Gatto D, Pasha L and Parrella B, ‘*Instagram and counterfeiting in 2019: new features, old problems*’ (9 April 2019)

The International Anticounterfeiting Coalition, *‘Counterfeiting costs everyone’* <https://www.iacc.org/resources/about/what-is-counterfeiting> accessed 15 August 2019

University of Copenhagen, ‘New weapon to combat counterfeit goods: use your smartphone to check for fake merchandise’ (Science Daily, 21 February 2019) <https://www.sciencedaily.com/releases/2019/02/190221111717.htm> accessed 1 June 2019

World Health Organisation, ‘Substandard and falsified medical products’ (31 January 2018) <https://www.who.int/en/news-room/fact-sheets/detail/substandard-and-falsified-medical-products> accessed 15 July 2019

World Health Organization, ‘WHO Global Surveillance and Monitoring System for substandard and falsified medical products’ (Geneva, 2017)