Intermediary Liability and Takedown Policies in Asia

Prepared by the Digital Asia Subcommittee of the Internet Committee

November 3, 2021

New York | Beijing | Brussels | Washington, D.C. | Singapore | Santiago

PowerfulNetworkPowerfulBrands®

Contents

Intro/ Summary

The Digital Asia Subcommittee of the INTA Internet Committee 2020-2021 research team conducted a survey with practitioners in sixteen Asia-Pacific jurisdictions to collect information and provide an analysis regarding intermediary liability and takedown practices. The information gathered through the survey research discusses the general legal framework, including laws governing e-commerce and forthcoming changes in these jurisdictions. The material also examines the liabilities of intermediaries including e-commerce entities, potential defenses available to them, as well as aspects such as disclosure of user data and takedown policies, obligations, and procedures. The Internal Research and Communications Subcommittee 2020-2021 has collated this research to produce a document intended to provide a quick overview of the position in each of these sixteen jurisdictions and general trends followed.

The legal framework governing e-commerce in these Asia-Pacific jurisdictions is generally based on a combination of intellectual property laws, consumer protection laws, and data protection and privacy laws. The framework naturally varies from jurisdiction to jurisdiction, some of which have additionally codified specific legislations covering e-commerce/information technology/electronic transactions, such as Japan's Act on Electronic Signature and Certification Business and Unfair Competition Act.

Platform operators across the board potentially face liability in instances of violation of intellectual property rights particularly copyright violation, consumer protection rights, and data privacy. However, in virtually all the surveyed jurisdictions, platform owners have the benefit of an intermediary liability exemption particularly in the absence of knowledge of the unlawful activity coupled with general compliance with other legal requirements. E-commerce sellers on the other hand may be more directly liable for violations and the benefit of 'intermediary' defenses afforded to them are more curtailed and limited as compared to platform owners. Secondary liability of platform operators also exists, particularly if the unlawful activity is not addressed upon gaining knowledge thereof. The threshold of 'having knowledge' however varies from jurisdiction to jurisdiction.

The survey further reveals that the obligation on platform operators to comply with data protection and consumer protection laws, generally precludes brand owners from asking for user details as a matter of right. Courts however are empowered to pass orders for disclosure of such information when deemed necessary.

Platform operators ordinarily have effective takedown policies in place to assist brand owners in taking down either inherently objectionable material or content found to be violative by a competent court. The general standard for take down usually involves either a notification from the brand owner or a court order, following which the platform operator is required to take down the content within a specified timeframe. In some cases, platform operators are required to provide an opportunity to the content owner/uploader to dispute the notification given by the brand owner by way of a counter notification. Some of these jurisdictions require the intermediaries to evaluate the notification and counter notification and thereby play an adjudicatory role for take down of the content in question.

Overall, while this document may serve as a valuable starting point for any inquiry into intermediary liability of a specified jurisdiction, it is recommended that a qualified local attorney should be consulted for specific advice, and neither INTA nor the Internet Committee can guarantee its accuracy. The Internet Committee wishes to thank the practitioners for their contribution and efforts.

Australia

Contributor: Kimberley Evans, Allens Patent & Trade Mark Attorneys

No.	Main Points	Answer
1.	Discussion on the general legal framework and scope of the laws governing e-commerce	The liability of e-commerce platforms for third party (seller) content in Australia lacks coherency as there is no one piece of legislation that governs e-commerce. Under Australian law, intermediary liability in e-commerce is largely dealt with by the *Copyright Act 1968* (Cth), which provides specific provisions dealing with intermediary liability. While the *Australian Consumer Law* and the *Trade Marks Act 1995* (Cth) have potential to be used against intermediaries but there are inherent difficulties in meeting the requirements for misleading and deceptive conduct or trade mark infringement. **Copyright Act** The *Copyright Act 1968* (Cth) creates a system of secondary liability, expressly providing that infringement occurs if a person authorises an infringing act (for example, under s36(1)). E-commerce websites have been held liable for 'communicating' works that infringe copyright and for authorising infringement. However, part V div 2AA of the *Copyright Act* protects 'service providers' from copyright infringement in certain circumstances. This includes carriage service providers; organisations assisting persons with disabilities; bodies administering public libraries; and bodies administering archives, key cultural institutions or educational institutions. Copyright owners cannot seek monetary damages against these organisations for copyright infringement resulting from: • Providing facilities/services for transmitting, routing, or providing connections for the copyright material; • Automatic caching of copyright material; or • Referring users to an online location. **Australian Consumer Law**

		The *Australian Consumer Law* generally prohibits misleading and deceptive conduct in the course of trade. Liability for misleading and deceptive conduct is strict, but requires actual wrongful conduct on the part of the defendant that is likely to mislead or deceive. There is no separate secondary head of liability. The Australian courts have considered whether the *Australian Consumer Law* can be used against intermediaries who publish another person's misrepresentation or statement that constitutes misleading and deceptive conduct. While the *Australian Consumer Law* provides remedies for accessorial liability where a person has been involved in misleading and deceptive conduct, there have not been any successful cases against intermediaries to date. For example, in *Google Inc v ACCC* (2013) 249 CLR 435, the High Court confirmed that where the publisher of a message is a 'mere conduit', the publisher is not liable. Liability under the *Australian Consumer Law* will only be found where the intermediary has conveyed the message in circumstances where it would be seen by the public as having adopted or endorsed the representation or conduct. **Trade Marks Act** The *Trade Marks Act 1995* (Cth) does not contain any provisions that specifically deal with intermediary liability but the infringement provisions of the Act may be utilised if a trade mark owner can overcome the difficulty in showing that an online service provider has used the trade mark in a trade mark context.
2.	What intermediary liabilities do the platform operators hold? (Discussion on the possible liabilities faced by platform operator i.e. contractual liabilities, personal data protection or intellectual property. Please include if there are any defences available for intermediaries.)	The *Copyright Act 1968* (Cth) is the only piece of legislation to expressly attribute liability to an e-commerce platform where that platform has authorised an infringing act. E-commerce websites have been held liable for 'communicating works' that infringe copyright and for authorising infringement by selling items that infringe another party's copyright. For example: • *In Hells Angels Motorcycle Corporation (Australia) Pty Ltd v Redbubble Ltd* (2019) 140 IPR 172, the Federal Court held that Redbubble (an e-commerce platform) had communicated the copyright work (primary infringement); it also noted secondary infringement would be made out.

		• In *Pokémon Company International, Inc. v Redbubble Ltd* [2017] FCA 1541, Redbubble was also found liable for both directly infringing copyright and for authorising infringement by its users. However, these cases emphasise that platform operators will only be liable where they have been found to authorise copyright infringement (that is, the platform operator has enabled others to infringe copyright).
3.	Whether brand owners have the right to request/demand for disclosure of the details of the alleged infringers (including, name, contact details, address, bank details) from the platform operators. (Discussion should include the relevant grounds for the request/demand, impact of personal data protection laws, the governing laws and regulations and the defences available for the platform operators)	There is nothing under Australian law to prevent a brand owner from contacting an alleged infringer directly (through an e-commerce platform) to request personal information. However, there is nothing to compel a platform operator to provide those details and most privacy policies for e-commerce platforms would prevent the disclosure of personal details by the platform operators. In addition, the *Privacy Act 1988* (Cth) (which applies to businesses with turnover greater than A$3 million and some types of small businesses) will generally prevent the disclosure of personal information without the permission of the individual or a court order. Brand owners wishing to obtain the personal details of alleged infringers from e-commerce platform operators must obtain a court order for preliminary discovery against another person or entity to help the brand owner ascertain the identity or description of a prospective respondent. However, it may be difficult for brand owners to obtain such a court order as the Federal Court's power to grant an order for preliminary discovery is discretionary, even where the brand owner has been able to establish that the brand owner: 1. may have a right to obtain relief against a person; 2. is unable to identify that person; and 3. can prove that a third party (the subject of the requested discovery order) can help identify that person. See *Dallas Buyers Club LLC v iiNet Limited* [2015] FCA 317.
4.	What are the general applicable laws and the scope in relation to takedown policies? (Related laws/regulations/directions/order and its applicability as well as domain name	If a brand owner believes that content on a website infringes their intellectual property rights or constitutes misleading and deceptive conduct in contravention of the *Australian Consumer*

	registration policies to takedown policies of IP rights)	*Law*, the brand owner can send a letter of demand to the website operator and demand that the operator take down the infringing or contravening content. Schedule 2 of the *Copyright Regulations* provides a number of forms that may be used to notify service providers (including e-commerce platforms) that infringing materials are being hosted, displayed or stored on a particular website. The *Copyright Act* and the *Copyright Regulations* provide for 3 take-down procedures using prescribed forms. • The first applies where a copyright owner or their agent believes on reasonable grounds that material hosted by the service provider is infringing their copyright (***Owner Notice***) (regs 23-28). • The second applies where a service provider otherwise becomes aware of material hosted by them that is or is likely to be infringing copyright (regs 29-32) (***SP Initiated Takedown***). • The third applies in relation to search or linking service providers, where the copyright owner or their agent believe on reasonable grounds a reference or link to material is infringing (regs 33-35) (***Link Notice***). Generally, service providers are required to act expeditiously to remove or prevent access to the site after a takedown notice is issued. The procedures for the three forms of take-down vary, with key differences in the service providers' obligations and whether the user who requested the service provider to host/link the material (***Third Party User***) is given an opportunity to respond to the takedown notice. If the website operator refuses to remove the content, the brand owner would need to obtain a court order under the relevant Act (*Trade Marks Act, Copyright Act, Australian Consumer Law*) for the content to be taken down. ***.au Domain Name policies*** au Domain Administration Ltd (***auDA***) is the administrator and self-regulatory policy body for the .au ccTLD. auDA will not mediate or resolve disputes between a registrant and another party over a domain name, except insofar as the dispute involves a breach or possible breach of an auDA published policy. auDA specifically

		states that it does not have jurisdiction to handle complaints relating to possible breaches of the *Australian Consumer Law, Copyright Act 1986, Trade Marks Act 1995, Privacy Act 1988* or any other legislation: see paragraphs 3 and 7 of 2015-01 *Complaints Policy*.
5.	What takedown obligations do the e-commerce sellers have? (Discussion on e-commerce sellers' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	E-commerce sellers will be bound by the terms and conditions of any e-commerce platform on which they operate and more generally by the provisions of the *Australian Consumer Law, Copyright Act 1968* and *Trade Marks Act 1995*. However, if the e-commerce seller's conduct is not captured by the policies of the relevant e-commerce platform, the brand owner would be required to obtain a court order under the *Australian Consumer Law* or *Trade Marks Act 1995* in order to have the infringing content taken down. In relation to copyright, takedown notices may be issued under the *Copyright Act* against sellers who infringe copyright (see above under question 4). After receiving a takedown notice or becoming aware of likely infringing material, service providers must act expeditiously to remove or disable access to the relevant material, or, in the case of search or linking providers, the reference or link to the relevant material. In the case of an Owner Notice, the service provider must notify the Third Party User (typically in this circumstance, a seller) of the notice. The Third Party User may issue a counter-notice within three months to dispute the claim. If they issue a counter-notice, the service provider must notify the copyright holder and inform them they have 10 days to initiate an action in court. If the copyright holder does not do so, or otherwise informs the service provider they have discontinued the action or were unsuccessful, then the service provider must restore the material. Where service providers become aware that the material is or is likely to be infringing, the service provider must act expeditiously to remove or disable access to the material, and notify the Third Party User/seller. The Third Party User is able to have their material restored if they successfully issue a counter-notice within three months. This must satisfy the service provider that the user believes in good faith the service provider's removal of the material was based on an incorrect identification of the material or a

		mistake as to fact or law, and the user's grounds for those beliefs. If a Third Party User knowingly makes a material representation in their counter-notice, they can be sued for any resulting loss or damage: reg 39. It is worth noting this also applies to a copyright owner who makes a misrepresentation in issuing a takedown notice.
6.	What takedown obligations do the platform operators have? (Discussion on the platform operators' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	All platform operators must comply with any court orders that require content to be taken down. In relation to copyright infringement, as outlined above, platform operators generally must expeditiously remove material after receiving a takedown notice from a copyright owner, or where the service provider becomes aware that material is infringing or likely to be infringing. In the case of Owner Notices and SP Initiated Takedowns, the platform operators must notify Third Party Users about the removal of the content and give them an opportunity to reply with a counter-notice. Platform operators are obliged to restore the material if a counter-notice by the Third Party User is successful. If they do not restore the material, the platform operator may be liable for damages or other civil remedies against the Third Party User: reg 38. Platform operators are not obliged to notify Third Party Users about a Link Notice as there is no opportunity to respond with a counter-notice.
7.	Discussion on the takedown procedure i.e the procedures / steps.	The steps for issuing takedown notices under the Copyright Regulations are: A. Owner Notice 1. The copyright owner/rightsholder issues a takedown notice to the service provider; 2. The service provider must expeditiously remove or disable access to the copyright material; 3. The service provider notifies the Third Party User of the copyright content and their right to issue a counter-notice; 4. The Third Party User may give a counter-notice in the prescribed form disputing the claims in the takedown notice. a. If the Third Party User does not issue a counter-notice,

		the service provider is not required to do anything further. The material does not get restored. b. If the Third Party User does issue a counter-notice, the service provider must send the counter-notice to the copyright owner who issued the takedown notice. They must also send a notice stating that the service provider will restore access to the copyright material unless the copyright owner brings an action in court relating to the infringing behaviour. 5. If the copyright owner does not bring such an action within 10 days, or notifies the service provider that the action for infringement was discontinued or unsuccessful, the service provider must restore the copyright material as soon as practicable. B. SP Initiated Takedown 1. The service provider must act expeditiously to remove or disable access to the material; 2. As soon as practicable, it must notify the Third Party User that the material has been removed, and the grounds for removal; 3. Counter-notice: a. If the Third Party User does not issue a counter-notice, the service provider is not required to do anything further. The material does not get restored. b. The Third Party User may issue a counter-notice within three months in the prescribed form, stating that they believe in good faith that the removal was based on incorrect identification of the material, or on a mistake of fact or law, and the grounds for this belief.

		4. If, following the counter-notice, the service provider is satisfied that the material is not, or is not likely to be infringing, they must restore the material. C. Link Notice 1. The copyright owner/rightsholder issues a takedown notice to the search or linking service provider in the prescribed form; 2. The service provider must expeditiously remove or disable access to the reference or link to the copyright material. There is no requirement to inform the Third Party User.
8.	Are there any forthcoming changes to the law / regulations in relation to intermediary liability / takedown policies / practices?	None currently under discussion.
9.	General comments on the current legal framework (Are there any interesting case studies or identified problems/issues).	N/A

Cambodia

Contributors: Thomas Treutler of Tilleke & Gibbins; Jay Cohen / Chandavya Ing of Tilleke & Gibbins (Cambodia) Ltd.
Coordinator: Timothy Siaw of Shearn Delamore & Co.

No.	Main Points	Answer
1.	Discussion on the general legal framework and scope of the laws governing e-commerce.	The Law on Electronic Commerce (E-commerce Law) was enacted on November 2, 2019. The stated purpose of the law is to manage domestic and cross-border e-commerce activities in Cambodia, establish legal certainty for electronic transactions, and provide confidence to the public in using electronic communications. The E-commerce Law broadly applies to all acts, documents, and commercial and civil transactions executed via an electronic system, except those that are related to powers of attorney, wills and successions, and real estate, and others as defined by further regulations. Given the broad scope of the law, its reach could potentially extend to offshore entities as well, though it is anticipated that further implementing *Subdecrees* will clarify this point. Therefore, it is necessary to monitor whether other types of transactions are excluded from the scope of the E-commerce Law.
2.	What intermediary liabilities do the platform operators hold? (Discussion on the possible liabilities faced by platform operator i.e. contractual liabilities, personal data protection or intellectual property. Please include if there are any defences available for intermediaries.)	The E-commerce Law provides a safe harbor defense / immunity for intermediaries whereby they are not liable for information contained in the electronic records related to their service provision if: (1) The intermediary is not the one who sent such a record; and, (2) The intermediary does not have any actual knowledge or is not aware of any facts or circumstances that leads to knowledge that the content may give rise to civil or criminal liability; or, (3) The intermediary becomes aware afterwards of information, facts, or circumstances that may lead to civil or criminal responsibility and the e-

		commerce intermediary complies with all mandatory content removal procedures (e.g., removing the content and informing the relevant governmental authority). However, notwithstanding the above safe harbour defence, intermediaries would still be liable for any obligations pursuant to any contracts, other applicable laws, existing regulations, or orders of any courts or competent authorities. Intermediaries also have specified obligations towards information or incidents that could lead to civil or criminal responsibility by having to carry out takedown measures as defined under Article 25 of the E-commerce Law. Failure to carry out those content removal procedures could lead to imprisonment from one month to one year and a fine from KHR 100,000 to KHR 2,000,0000 (approximately USD 25 to USD 500). To the extent that intermediaries take good faith actions based on orders from the Ministry of Posts and Telecommunications (**MPTC**) or other competent institutions, intermediaries are insulated from civil liability that may arise under law or contract. Article 27 of the E-commerce Law requires intermediaries to comply with codes of professional ethics; however, such codes have not yet been enacted. Although Cambodia has not yet enacted any specific data protection laws or regulations, an intermediary must comply with data protection provisions under the E-commerce Law, which requires an intermediary to protect data in all reasonable circumstances to avoid loss, access, use, modification, leakage, or disclosure of such personal information, unless authorized by information owners or authorized parties. Failure to abide by these requirements can subject an authorized intermediary to imprisonment from one year to two years and a fine from KHR 2,000,0000 to KHR 4,000,000 (approximately USD 500 to USD 1,000). While there are no specific provisions under any intellectual property-related laws on intermediary liability, in general, an infringement of intellectual property rights, including trademarks, patents, utility model certificates, industrial designs, and copyrights

		in Cambodia could lead to civil or criminal liability.
3.	Whether brand owners have the right to request/demand for disclosure of the details of the alleged infringers (including, name, contact details, address, bank details) from the platform operators. (Discussion should include the relevant grounds for the request/demand, impact of personal data protection laws, the governing laws and regulations and the defences available for the platform operators)	Under Cambodia's intellectual property framework, there are no specific laws that address online counterfeiting and what information can be obtained from platform operators or other intermediaries. Under the E-commerce Law, there is no explicit obligation to provide or disclose the details of the alleged infringers to brand owners whose trademark rights are being infringed. The platform operator only needs to store such information and notify the MPTC, and relevant ministries or institutions of the identity of the alleged infringer. As the platform operators, they has an obligation to comply with data protection provisions under the E-commerce Law, which requires them to protect data in all reasonable circumstances to avoid loss, access, use, modification, leakage, or disclosure of such personal information, unless authorized by information owners or authorized parties. Such data protection requirements may run counter to a brand owner's desire to obtain information about a potential infringer. However, this does not mean that the platform operators will not cooperate with brand owners in combating online infringements of intellectual property rights. In practice, the most popular online marketplaces or social media platforms provide takedown mechanisms to help prevent online infringement of intellectual property rights. With this mechanism available, brand owners could follow the platform's required steps in order to report the infringement and to request for removal of the infringing content.
4.	What are the general applicable laws and the scope in relation to takedown policies? (Related laws/regulations/directions/order and its applicability to takedown policies of IP rights)	The only law that addresses takedown policies is the E-commerce Law. As discussed above, Article 25 of the E-commerce Law requires intermediaries or electronic-commerce service providers to remove information, to stop providing services related to that information, to store the information as evidence, and to notify MPTC and relevant competent authorities if they are aware of information that may lead to civil or criminal liabilities. While there are no specific provisions on takedown measures under Cambodia's intellectual property related laws, infringement

		of intellectual property rights could lead to civil or criminal liability. Therefore, the takedown policies under the E-commerce Law would be applicable to enforcing intellectual property rights as civil and criminal liability for infringement is created under Cambodia's intellectual property related laws.
5.	What takedown obligations do the e-commerce sellers have? (Discussion on e-commerce sellers' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	Under the E-commerce Law, e-commerce sellers could be classified as "e-commerce service providers," because they use electronic means to supply goods or services. Electronic-commerce service providers are defined as persons using electronic means to supply goods or services, except for insurance institutions As such, they would have the same takedown obligations as intermediaries under Article 25 of the E-commerce Law. Those obligations include the obligation to remove the information, stop providing services related to such information, store the information as evidence, and notify the MPTC and relevant competent authorities of the facts and identity of the alleged infringers. Moreover, they also have to take actions relating to the takedown as ordered by the MPTC or competent ministries or institutions. These takedown obligations will be illustrated further in Question 6 below. In term of intellectual property rights, the persons using electronic communication to sell goods or services need to make sure that they are not using any registered marks or confusingly similar marks thereof without authorization from the brand owners.
6.	What takedown obligations do the platform operators have? (Discussion on the platform operators' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	The takedown obligations of platform operators will depend on where the information is located and the nature of the information. If the information is in their records, the platform operator must remove such information from the information system under its management and stop providing services related to such information. Platform operators also must store the information as evidence and notify the MPTC and relevant competent ministries or institutions of the facts and the identity of the alleged infringers. If there is an incident or situation that could lead to such civil or criminal liabilities, the platform operators must store the information as evidence and notify the MPTC and relevant

		competent ministries or institutions of the facts and the identity of the alleged infringers. The platform operators must also remove the infringing information from their information system, postpone or stop providing services to that person or postpone or stop providing services related to that electronic record, as ordered by the MPTC or competent ministries or institutions. However, as discussed in Question 2 above, platform operators are protected by a safe harbour defence / immunity when acting in good faith on orders of the MPTC or competent ministries or institution.
7.	Discussion on the takedown procedure i.e the procedures / steps.	Article 25 of the E-commerce Law sets out the below takedown procedure. Upon becoming aware of the information in the electronic records that may lead to civil or criminal liability, the intermediary must: • remove the information from the information system under their management and stop providing services related to such information; and • store the information as evidence and notify the MPTC and relevant competent ministries, institutions of the facts and identity of the alleged infringers. If the intermediary becomes aware of any incident or situation leading to civil or criminal liability, the intermediary shall store the information as evidence and notify the MPTC and relevant competent ministries or institutions. If the MPTC or relevant competent ministries or institutions become aware of (either by way of the above notification or otherwise) information in the electronic records that may lead to civil or criminal liability, they could order the intermediary to: • remove the information from the information system under their management; • postpone or stop providing services to that person; or

		• postpone or stop providing services related to electronic records.
8.	Are there any forthcoming changes to the law / regulations in relation to intermediary liability / takedown policies / practices?	The E-commerce Law gives power to the Ministry of Commerce and the MPTC as well as other relevant authorities to create a so-called "code of professional ethics for intermediaries and electronic-commerce service providers" and an inter-ministerial *Prakas* on electronic commerce. If such a code of conduct is established or if such a *Prakas* is enacted, there may be more detailed provisions on intermediary liability and takedown policies.
9.	General comments on the current legal framework (Are there any interesting case studies or identified problems/issues).	The E-commerce Law was signed on November 2, 2019; however, it was only put into implementation six months after it entered into force, being June 2, 2020. Therefore, there is little practical experience with the law up until the date of this answer. Moreover, several regulations and mechanism swill have to be enacted and established in order to fully implement the law. Therefore, while the law is in force, it has not been fully implemented in practice. That said, businesses should not overlook the law and should familiarize themselves with the law and watch out for additional implementing regulations. In the meantime, brand owners should also make use of the mechanism relating to the takedown request of infringing content, which is made available by several populous online platforms.

India

Contributors: Aditya Gupta (Ira Law); Shivangi Narang (L&L Partners)

No.	Main Points	Answer
1.	Discussion on the general legal framework and scope of the laws governing e-commerce	The liability of e-commerce platforms for third party (seller) content is regulated by India's Information Technology Act. Section 79 of the Information Technology Act provides e-commerce platforms immunity from liability, subject to fulfilment of certain conditions (explained in detail below). The Act extends such protection only in those instances where the intermediary does not play any part in creation or modification of the data or information. It is also contingent on the intermediary removing any unlawful content on its computer resource on being notified by the appropriate Government or its agency or upon receiving actual knowledge (as detailed herein under serial no. 2) Recently, the Indian Government has also notified Consumer Protection (E-commerce) Rules, 2020 which require that e-commerce platforms must adhere to fair trade practices and also mandate that complete contact details of sellers on such platforms are known to buyers.
2.	What intermediary liabilities do the platform operators hold? (Discussion on the possible liabilities faced by platform operator i.e. contractual liabilities, personal data protection or intellectual property. Please include if there are any defences available for intermediaries.)	Platform operators are potentially liable under the following laws: 1. Liability for IP infringement 2. Liability under the consumer protection law 3. Liability under contract law **Liability for IP infringement**: E-commerce platform operators are potentially liable for IP infringement if they fail to fulfil the pre-conditions for availing the immunity from liability under Section 79 of the Information Technology Act, 2000 ('IT Act'). If these pre-conditions are not fulfilled, an e-commerce platform operator can be liable for both injunction and damages as if it had committed the infringing act itself.

		The Information Technology Act mentions three pre-conditions for availing the immunity from liability, namely: (a) the function of the intermediary must be limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or (b) the intermediary must not - (i) initiate the transmission, (ii) select the receiver of the transmission, and (iii) select or modify the information contained in the transmission; (c) the intermediary observes due diligence while discharging his duties under the Act and observes such other guidelines as the Central Government may prescribe in this behalf. Further the Central Government, in exercise of its powers under Section 79 of the IT Act, notified the Information Technology (Intermediaries Guidelines) Rules, 2011 which amongst others lays down the standard for "due diligence" to be met by an intermediary to take benefit of the safe harbour. Amongst these standards, is the requirement that the intermediary take down any information that "violates any law for the time being in force" or "infringes any patent, trade mark, copyright or other proprietary rights", within thirty six hours of receiving actual knowledge of the same from an affected person. This provision has been interpreted by the Supreme Court to mean that the "actual knowledge" must be knowledge of a Court order and not merely knowledge of a complaint by an affected party. In addition to the above three pre-conditions, an intermediary must also ensure the following for availing such immunity from liability: (a) the intermediary has not conspired or abetted or aided or induced, whether

		by threats or promise or otherwise in the commission of the unlawful act; (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner. This provision has been interpreted by the Supreme Court to mean that the "actual knowledge" must be knowledge of a Court order and not merely knowledge of a complaint by an affected party. In the context of e-commerce platforms, the Delhi High Court in *Amway Seller Services Pvt. Ltd.v. Amway India Enterprises Pvt. Ltd.* has found that: (i) when a potential customer accesses the site and takes the relevant action for making a purchase, it is the customer who is initiating the transmission. (ii) Further, the receiver of the transmission is the buyer, which should not be selected by the e-commerce operator. (iii) Further, e-commerce platform operator should not modify the information contained in the transmission, such as the choice of the product, the number of units, and so forth. **Liability under the consumer protection law**: E-commerce platforms potentially face liability under the Consumer Protection (E-commerce) Rules, 2020 for engaging in unfair trade practices and for failure to display and maintain seller-related information. Under this law, the e-commerce operator can be compelled to cease the unfair trade practice as also pay damages for engaging in this practice. **Liability under contract law**: e-commerce platform operators usually have contractual obligations to the buyers on the platforms. However, for most such obligations, they are

		indemnified by the seller where they incur any liability on account of any illegal act of the seller.
3.	Whether brand owners have the right to request/demand for disclosure of the details of the alleged infringers (including, name, contact details, address, bank details) from the platform operators. (Discussion should include the relevant grounds for the request/demand, impact of personal data protection laws, the governing laws and regulations and the defences available for the platform operators)	Under the Consumer Protection (E-commerce) Rules, 2020, e-commerce platform operators are obligated *inter alia* to prominently display on the e-commerce website details of the seller such as their name, address, customer care number, including ratings/feedback, terms and conditions generally governing its relationship with sellers on its platform including description of any differentiated treatment; modes of payment methods, etc. A customer can also seek information such as addresses or all branch offices and head office, website address and email address by making a request in writing. Failure to provide such information will likely amount to an unfair trade practice and may lead to liability under the Consumer Protection (E-commerce) Rules, 2020. Brand owners do not have any specific right to request/demand for disclosure of the details of the alleged infringers. However, in cases where brands owners have often sought such details in lawsuits against e-commerce platform operators, Courts have compelled e-commerce platform operators to disclose such details to the brand owners. The information provided usually includes the names, contact details and addresses of the alleged infringers. In cases where the infringement is egregious or of a serious nature, Courts have also compelled disclosure of bank account details of the alleged infringers. The question of impact of personal data protection laws by such disclosure has not yet been considered by Indian Courts.
4.	What are the general applicable laws and the scope in relation to takedown policies? (Related laws/regulations/directions/order and its applicability as well as domain name registration policies to takedown policies of IP rights)	An intermediary is liable to takedown content which is unlawful, either upon (i) receiving "actual knowledge" of such unlawful content from entities such as brand owners/ copyright owners; or (ii) upon receiving a notification from the appropriate agency in the Government. This provision was interpreted by the Indian Supreme Court (see *Shreya Singhal versus Union of India*) to mean that the actual knowledge of such unlawful content from private entities must be pursuant to a Court order. In other words, the private entities must

		first approach the Court to obtain an order stating that the content is unlawful and the intermediary would be liable for taking down the content only upon receipt of a Court order. This requirement of a Court order has however been diluted in the context of copyright infringement wherein a two-Judge bench of the Delhi High Court (see *MySpace Inc. versus Super Cassettes Industries Pvt. Ltd.*) has found that notification by a copyright holder is sufficient to constitute actual knowledge and trigger the takedown obligation. The Delhi High Court stated that the requirement of a Court order as stipulated in *Shreya Singhal* will not apply to copyright cases. It is, however, important for the copyright owner to specifically identify the infringing content by means of identifying the URL (Uniform Resource Locator) where the infringing content is located. A generalized knowledge that infringing material is present on the platform is insufficient to trigger the takedown obligation. Several e-commerce platforms such as Amazon and Flipkart have formulated their own IP infringement policies. These policies do not require brand owners to furnish a Court order and these e-commerce platforms act on the basis of a notification of an infringing listing from a brand owner. **Indian Courts exercising long-arm jurisdiction in respect of take down of content:** In this regard, it is pertinent to note a recent decision of the Single Judge of the Delhi High Court in *Swami Ramdev & Anr*. v. *Facebook, Inc. & Ors*., wherein the plaintiffs had filed the suit against media/ technology companies including Facebook, Google, YouTube and Twitter seeking a global take down order for certain defamatory content that was available on these platforms. The Court in this case observed that as per the language in Section 79(3)(b) of the IT Act, intermediaries were under an obligation to remove content from their platforms once ordered by a competent court. Such content was to be removed from the 'computer resource' controlled by the intermediary. Since the definition of 'computer resource' under the IT Act includes "computer network" within its ambit, the court concluded that the obligation to take down content should be from the entire network of computers. The Court also relied on Section 75 of the IT Act

		(which provides extra territorial application of the IT Act) and observed that if either the uploading of objectionable content takes place from India or the information/data is located in India on a computer resource, Indian courts would have the jurisdiction to pass global injunctions. The Court accordingly ordered the defendants to take down, remove block, restrict/ disable access, on a global basis, to all the defamatory content, which had been uploaded from I.P. addresses within India and for content which was uploaded from outside India, the defendants were directed to block access and disable them from being viewed in the India and ensure that users in India are unable to access the same. An appeal filed against the said decision is currently pending, with the effect of the order being stayed.
5.	What takedown obligations do the e-commerce sellers have? (Discussion on e-commerce sellers' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	There is no specific law governing the takedown obligations of e-commerce sellers. Sellers are liable for the products listed by them and do not enjoy the status of an intermediary. Thus, a seller can be called upon to takedown an unlawful listing (whether under IP law or otherwise) through the means of a legal notice. This notice may even require the e-commerce seller not to place unlawful listings in future. If the seller does not take down the listing based on a legal notice, a Court can be approached for an injunction as well as damages. The Court may pass an injunction against an e-commerce seller not only to takedown the specific listings identified by the Plaintiff, but also restrain the e-commerce seller not to place such infringing listings in future.
6.	What takedown obligations do the platform operators have? (Discussion on the platform operators' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	An intermediary is liable to take down content which is unlawful, either upon (i) receiving "actual knowledge" of such unlawful content from private entities such as brand/ copyright owners; or (ii) upon receiving a notification from the appropriate agency in the Government. Regarding actual knowledge of unlawful content from private entities, the private entity must send a notification pursuant to a Court order finding the content to be unlawful. An exception in this regard has been recognized in cases relating to copyright infringement, wherein a notification by the

		copyright holder is sufficient to trigger the takedown obligation. The intermediary is liable to respond to the takedown request within a period of 36 hours from its receipt. Courts in India have also recognized that platform operators do not have a "monitoring obligation" i.e. they cannot be expected to monitor or filter illegal content on their platforms. Illegal content is required to be specifically identified by the injured party, including by means of identifying the specific URL, and only the specific URLs are required to be taken down by the platform operator. Where the intermediary fails to takedown the content in accordance with the above, the intermediary can no longer avail the immunity from liability of the third party content and may be found liable under the relevant law for publishing/ distributing/ communicating the infringing content.
7.	Discussion on the takedown procedure i.e the procedures / steps.	The pre-requisites for a valid takedown notice: 1. Under laws other than copyright: a. The takedown notice must be sent pursuant to a Court order finding content to be unlawful; b. The takedown notice must identify the specific content (by means of URLs) which is available on the platform which falls within the scope of the Court order. 2. Under copyright law: a. The takedown notice must be sent by the right holder; b. The notice must identify the specific infringing content (by means of URLs) which is available on the platform. Upon receipt of a valid takedown notice, the intermediary is liable to respond to the takedown request within a period of 36 hours from its receipt. The intermediary is required to take measures to refrain from facilitating such access for a period of twenty-one days from the date of receipt of the complaint or till he receives an order from the competent

		court restraining him from facilitating access whichever is earlier.
8.	Are there any forthcoming changes to the law / regulations in relation to intermediary liability / takedown policies / practices?	The Government of India had proposed significant amendments to the rules governing intermediary liability in year 2018. Some of the key changes that are proposed under the said draft rules are: 1. intermediaries may be required to provide assistance to government agencies (based on a lawful order), within 72 hours of communication requesting such assistance and intermediaries shall be under an obligation to enable tracing of the originator of the information on its platform, as required by the government agencies; 2. intermediaries with more than fifty lakh users or as notified by the government, are required to be incorporated in India, under the Companies Act, 2013, have permanent registered office with a physical address in India and appoint a senior designated functionary who is available for 24x7 coordination with law enforcement agencies; 3. On receiving actual knowledge through a court order or on being notified by the government, an intermediary will be under an obligation to remove or disable access to unlawful acts relatable to Article 19(2)1 of the Constitution of India, within 24 hours; and 4. The intermediary will be required to deploy technology-based tools for identifying and removing unlawful information or content. These amendments underwent several rounds of stakeholder consultations and have not yet been notified. Further, the Personal Data Protection Bill, 2019 ("the Bill") was tabled before the Indian Parliament by the Minister of Electronics and Information Technology on 11 December 2019. The said Bill is now being reviewed by a Joint Parliamentary Committee

[1] These are acts relating to the sovereignty of India, and integrity of India, security of state, ffriendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, on its computer resource without vitiating the evidence in any manner.

		in consultation with various groups. The Bill seeks to lay down certain norms in respect of data protection to be followed by "social media intermediaries", which definition would not include *inter alia* intermediaries which primarily enable commercial or business oriented transactions.
9.	General comments on the current legal framework (Are there any interesting case studies or identified problems/issues).	The law regarding intermediary liability in India is fast developing. One of the most significant decisions (Amazon Seller Services Pvt. Ltd. v. Amway) in the space of liability of e-commerce platforms for trademark infringement was passed in February, 2020 and the changes in the consumer protection law were passed in July, 2020. Several cases are pending in Court relating to obligations of e-commerce operators to ensure that trademark infringing products are not sold on their platforms. Another interesting issue which is currently being litigated in Courts is whether intermediaries providing platforms for User Generated Content (eg. Short video apps such as TikTok) are liable to introduce technological filters for ensuring copyrighted music is not uploaded on their platforms without the consent of the copyright owner. Note: The standards of intermediary liability of an e-commerce platform facilitating selling of pharmaceutical products is usually more stringent requiring such platforms to oblige with pharmaceutical laws as well. Pursuant thereto the Department of Health and Family Welfare published the Draft E-pharmacy Rules ('Draft Rules') on August 28, 2018 and invited comments from the public. The Draft Rules contemplate licensing of websites/platforms engaged in the online sale, offer for sale, stocking, distribution or exhibition of drugs. However, these rules have not been notified till date.

Indonesia

Contributor: **Thomas Treutler** / **Hani Wulanhandari** (Tilleke & Gibbins)
Coordinator: Timothy Siaw (Shearn Delamore & Co.)

No.	Main Points	Answer
1.	Discussion on the general legal framework and scope of the laws governing e-commerce.	The applicable laws are: - Indonesian Criminal Code; - Indonesian Law No.7 year 2014 on Trade; - Indonesian Law No. 8 of 1999 on consumer protection Law; - Indonesian Law No. 11 of 2008 on Electronic information and transactions; - Circular letter of Ministry of Communication and Informatics No. 5 of 2016 on Limitations and Responsibilities of Electronic Commerce Platform and Merchant Providers; - Government regulation no 80 year 2019 on electronic commerce.
2.	What intermediary liabilities do the platform operators hold? (Discussion on the possible liabilities faced by platform operator i.e. contractual liabilities, personal data protection or intellectual property. Please include if there are any defences available for intermediaries.)	The e-commerce holds secondary liability based on Articles 55 and 56 of the Indonesian Criminal Code. The law provides that anyone who deliberately provides an opportunity may also be liable for the act itself.
3.	Whether brand owners have the right to request/demand for disclosure of the details of the alleged infringers (including, name, contact details, address, bank details) from the platform operators. (Discussion should include the relevant grounds for the request/demand, impact of personal data protection laws, the governing laws and regulations and the defences available for the platform operators)	In Indonesia, unless there is a police complaint filed against a specific online seller the e-commerce is not obliged to disclose their user data information.
4.	What are the general applicable laws and the scope in relation to takedown policies? (Related laws/regulations/directions/order and its applicability to takedown policies of IP rights)	The applicable laws are: - Indonesian Criminal Code; - Circular letter of Ministry of Communication and Informatics No. 5 of 2016 on Limitations and Responsibilities of Electronic

		Commerce Platform and Merchant Providers ; - Government regulation no 80 year 2019 on electronic commerce.
5.	What takedown obligations do the e-commerce sellers have? (Discussion on e-commerce sellers' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	Sellers are not allowed to sell goods with misleading information or false information according to Consumer Protection Law. According to the Circular letter of Ministry of Communication and Informatics No. 5 of 2016 on Limitations and Responsibilities of Electronic Commerce Platform and Merchant Providers, the sellers must provide true and complete information for the product and/or services and comply with law and regulation, any content that sellers upload to e-commerce will be the seller's responsibility. However, there is no specific takedown obligation for the e-commerce sellers.
6.	What takedown obligations do the platform operators have? (Discussion on the platform operators' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	Circular letter of Ministry of Communication and Informatics No. 5 of 2016 on Limitations and Responsibilities of Electronic Commerce Platform and Merchant Providers, The platforms have to take action based on the report, including to verify the report, remove and/or block prohibited content, send notification to the merchant, provide feature for the merchant to clarify the report or refuse the report for any prohibited content including contents infringing intellectual property rights within 14 working days. For highly prohibited content the UGC platform provider must remove the content 1 (one) day after the report received.
7.	Discussion on the takedown procedure i.e the procedures / steps.	Each e-commerce platforms have different procedures for takedown request. Some provide a specific form, some do not provide any form and the takedown request can be sent as a request letter for takedown. In summary the steps are as follows: 1. To fill in the provided form (if any) or prepare a letter requesting for take-down together with the IP information in the form of a copy of the certificates. 2. Submit the form along with prove of IP ownership or send the respective e-commerce the request letter for takedown.

		3. Follow-up on the progress.
8.	Are there any forthcoming changes to the law / regulations in relation to intermediary liability / takedown policies / practices?	The government has just enacted the Government Regulation No. 80 year 2019 of Electronic Commerce (GR 80 year 2019) The GR came into force on 25 November 2019. However, a grace period of two years (due 25 November 2021) is provided to allow existing e-commerce to comply with the provisions. The GR 80 year 2019 regulates that an e-commerce provider is required to obtain a license. Also e-commerce operators are obliged to provide and store valid e-commerce transactions evidence. Furthermore, e-commerce and intermediary service operators are responsible for the consequences of negative/illegal content on their platforms. This responsibility will not apply if the e-commerce acts immediately to remove negative/illegal content once becoming aware both through its own monitoring system or based on a report from another party. The idea is to push the e-commerce to be more proactive in managing negative/illegal content on their respective platforms. Therefore, the government is imposing the responsibility. Violation of the provisions of GR 80 year 2019 would lead to administrative sanctions, in the form of: 1. warning letters 2. inclusion in a list of prioritized monitoring 3. inclusion in a black list 4. temporary suspension 5. revocation of business license Further provisions on the administrative sanctions will be governed in a ministerial regulation. However, we have not heard on when likely the ministerial regulation will be issued.
9.	General comments on the current legal framework (Are there any interesting case studies or identified problems/issues).	N/A

Macau

Contributor (Name+Firm) : **Bruno Nunes**, BN Lawyers
Coordinator (Name+Firm): Xianjie Ding, King and Wood Mallesons

No.	Main Points	Answer
1.	Discussion on the general legal framework and scope of the laws governing e-commerce	There are no specific laws concerning e-commerce. Hence, applicable regulations would be those that are foreseen in the Industrial Property Legal Act, in the Personal Data Protection Act and in the Commercial Code.
2.	What intermediary liabilities do the platform operators hold? (Discussion on the possible liabilities faced by platform operator i.e. contractual liabilities, personal data protection or intellectual property. Please include if there are any defences available for intermediaries.)	Platform operators would have contractual, personal data protection and intellectual property liabilities
3.	Whether brand owners have the right to request/demand for disclosure of the details of the alleged infringers (including, name, contact details, address, bank details) from the platform operators. (Discussion should include the relevant grounds for the request/demand, impact of personal data protection laws, the governing laws and regulations and the defences available for the platform operators)	Brand owners do not have such right.
4.	What are the general applicable laws and the scope in relation to takedown policies? (Related laws/regulations/directions/order and its applicability as well as domain name registration policies to takedown policies of IP rights)	The general applicable laws would be the Industrial Property Legal Act, in the Personal Data Protection Act and in the Commercial Code. There are no domain name registration policies.
5.	What takedown obligations do the e-commerce sellers have? (Discussion on e-commerce sellers' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	E-Commerce sellers would be obliged to takedown infringing listings if a court of law orders them to do so. That order would be issued either after a preliminary injunction or after a lawsuit. During both procedures, e-commerce sellers will be notified to provide their defence to the requests filed against them.
6.	What takedown obligations do the platform operators have? (Discussion on the platform operators' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	Platform operators would be obliged to takedown infringing listings if a court of law orders them to do so. That order would be issued either after a preliminary injunction or after a lawsuit. During both procedures, e-commerce sellers will be notified to provide

		their defence to the requests filed against them.
7.	Discussion on the takedown procedure i.e the procedures / steps.	1. Preliminary injunction or after a lawsuit filed and notified to the e-commerce seller or platform operator 2. E-commerce seller or platform operator can file their response 3. Trial Hearing 4. Court rules 5. Can be appealed.
8.	Are there any forthcoming changes to the law / regulations in relation to intermediary liability / takedown policies / practices?	No.
9.	General comments on the current legal framework (Are there any interesting case studies or identified problems/issues).	N/A

Malaysia

Contributor: **Timothy Siaw** (Shearn Delamore & Co.)

No.	Main Points	Answer
1.	Discussion on the general legal framework and scope of the laws governing e-commerce	There are several key legislations and regulations governing e-commerce in Malaysia. In particular:- a) Electronic Commerce Act 2006 ("**ECA**") The ECA is applicable to any commercial transaction conducted through electronic means including commercial transactions by the Federal and State Governments. Under the ECA, electronic messages are recognised and fulfils the legal requirements for formation of a valid contract between the parties. b) Electronic Government Activities Act 2007 ("**EGA**") The EGA provides for legal recognition of electronic messages in dealings and transactions between the Government and the public as well as the use of electronic messages to fulfil the legal requirements for the formation of a valid contract in Malaysia. c) Consumer Protection Act 1999 ("**CPA**") The CPA applies in respect of all goods and services that are offered or supplied to consumers in trade including trade transaction conduced through electronic means. Under CPA, provisions governing the protection of consumers in Malaysia are provided. This includes implied guarantees in respect of the supply of goods and services. d) Consumer Protection (Electronic Trade Transactions) Regulation 2012 ("**CPETTR**") The CPETTR came into force on 1 July 2013 and governs the operators that supply goods or services through a website or an online marketplace. Through the CPETTR, online marketplace operators are required to take reasonable steps to keep and maintain a record of names, telephone numbers and the address of the person who supplies goods or services in the online marketplace for a period of two (2) years. Further, the CPETTR imposes an obligation to disclose information as specified in the Schedule on the person who operates a business for the purpose of supply of goods or services through a website or in an online marketplace. This information includes the name of the person, the registration number, contact details, full price and the terms and conditions. e) Communications and Multimedia Act 1998 ("**CMA**")

		The CMA came into force on 1 April 1999 and regulates the converging communications and multimedia industries. The CMA and its subsidiary legislation apply both within and outside Malaysia. In particular, the CMA and its subsidiary legislation applies to any person beyond the geographical limits of Malaysia and her territorial waters if such person:- (i) is a licensee under this CMA; or (b) provides relevant facilities or services under the CMA in a place within Malaysia. f) Malaysian Communications and Multimedia Commission Act 1998 ("**MCM**") Established the Malaysian Communications and Multimedia Commission (MCMC). The MCMC is key regulator of the communications and multimedia industry based on the powers provided for in the CMA and MCM. The MCMC implements and promotes the Government's national policy objectives for the communications and multimedia sector as well as regulate the licensing of service providers on this sector. g) Digital Signature Act 1997 ("**DSA**") Digital signatures are vastly used to verify the identity of the sender of the electronic message as well as to verify the validity of the information contained therein. The DSA came into force on 1 October 1997 and regulates the use of digital signatures though the establishment of licensed Certification Authorities. h) Personal Data Protection Act 2010 ("**PDPA**") The PDPA governs the processing of personal data in commercial transactions in Malaysia and this includes processing of personal data for the purposes of e-commerce. The PDPA applies to any person who processes and any person who has control over or authorises the processing of any personal data in respect of commercial transactions. The PDPA does not apply to the Federal Government and State Governments or to personal data processed outside of Malaysia, unless the personal data is intended to be further processed in Malaysia. i) Direct Sales and Anti-Pyramid Scheme Act 1993 ("**DSAPSA**") Under Malaysian laws, any person carrying on direct sales business are regulated under the DSAPSA and are required to obtain a license. The DSAPSA similarly applies to sale through electronic transactions.
2.	What intermediary liabilities do the platform operators hold? (Discussion on the possible	Under Malaysian laws, there are no general legislations or regulations providing for intermediary liabilities. Platform operators are generally subject to obligations to comply with

	liabilities faced by platform operator i.e. contractual liabilities, personal data protection or intellectual property. Please include if there are any defences available for intermediaries.)	laws and regulations governing consumer protection, payment, advertising, protection of intellectual property rights, and other relevant laws in respect of the sale of goods or services. In particular, the platform operators are required to comply with intellectual property laws whereby there may be liability for sale of counterfeit goods or goods or services riding on the intellectual property rights of third parties. Upon request or direction from brand owners, e-platform operators would usually remove the infringing materials. Particularly, by order of the Courts, platform operators must take down such infringing listings and/or any information prohibited by laws. **Defences** Section 43C(1) of the Copyright Act 1987 ("**CA**") exempts a service provider from liability for copyright infringement if the infringement by its user occurs by reason of any of the following: (a) the transmission, routing or provision of connections by the service provider of an electronic copy of the work through its network; or (b) any transient storage by the service provider of an electronic copy of the work in the course of such transmission, routing or provision of connections. The exemption is, however, confined to any of the following situations: (a) the service provider did not initiate or direct the transmission of the electronic copy of the work; (b) the service provider did not select the electronic copy of the work but the transmission, routing or provision of connections was carried out through an automatic technical process; (c) the service provider did not select the recipient of the electronic copy of the work except as an automatic response to the request of another person; or (d) the service provider did not modify the electronic copy of the work other than as part of a technical process. Section 43D(1) of the CA provides that a service provider shall not be held liable for infringement of copyright for the making of any electronic copy of the work on its primary network if it is: (a) from an electronic copy of the work made available on an originating network; (b) through an automatic process; (c) in response to an action by a user of its primary network; or (d) in order to facilitate efficient access to the work by a user,

		provided that the service provider does not make any substantive modification to the contents of the electronic copy, other than a modification made as part of a technical process. Section 43E of the CA exempts a service provider from liability in the following situations: (a) when storing an electronic copy of a work where it is done at the direction of its user; and (b) when referring or providing a link or an information location service to its users where an electronic copy of the work is available at an online location of another network, provided that the service provider does not have knowledge of the infringing activity, does not receive any financial benefit directly attributable to the infringement and has responded promptly to a notification to take down the infringing copy.
3.	Whether brand owners have the right to request/demand for disclosure of the details of the alleged infringers (including, name, contact details, address, bank details) from the platform operators. (Discussion should include the relevant grounds for the request/demand, impact of personal data protection laws, the governing laws and regulations and the defences available for the platform operators)	There are no specific legislations or regulations which allows for brand owners to request or demand for disclosure of the details of the alleged infringers from platform operators. Brand owners will in practice request for disclosure of the information of the alleged infringers through the issuance of a cease and desist letter. However, platform owners are unlikely to comply with the request due to concerns with breach of the Personal Data Protection Act 2010 ("**PDPA**") and whether the act of disclosing information would affect the platform owner's commercial interest adversely. Under Section 7(1)(e) of the PDPA, a data user shall by written notice inform a data subject of the class of third parties to whom the data user discloses or may disclose the personal data. Consent for the disclosure must be obtained. Generally, civil laws allow for parties to request for pre-action discovery or discovery of documents or information during trial. Order 24 rule 7A (1) of the Rules of Court 2012 ("**ROC**") provides that an application for an order for the discovery of documents before the commencement of proceedings can be made by originating summons and the person against whom the order is sought shall be made defendant to the originating summons. Further, an application after the commencement of proceedings for an order for the discovery of documents by a person who is not a party to the proceedings shall be made by a notice of application, which shall be served on that person personally and on every party to the proceedings [Order 24 rule 7A (2) of the ROC]. An originating summons under Order 24 rule 7A of the ROC should include:- (a) the grounds for the application; (b) the material facts pertaining to the intended proceedings;

		(c) whether the person against whom the order is sought is likely to be party to subsequent proceedings in Court; (d) specify or describe the documents in respect of which the order is sought and show, if practicable by reference to any pleading served or intended to be served in the proceedings, that the documents are relevant to an issue arising or likely to arise out of the claim made likely to be made in the proceedings or the identity of the likely parties to the proceedings, or both, and that the person against whom the order is sought is likely to have or have had them in his possession, custody or power. Under Order 24 rule 3 of the ROC, subject to the provisions of this rule and of rules 4 and 8, the Court may at any time order any party to a cause or matter (whether begun by writ, originating summons or otherwise) to give discovery by making and serving on any other party a list of the documents which are or have been in his possession, custody or power and may at the same time or subsequently also order him to make and file an affidavit verifying such a list and to serve a copy thereof on the other party. A party to the suit may be ordered to discover for:- (a) the documents on which the party relies or will rely; and (b) the documents which could— (i) adversely affect his own case; (ii) adversely affect another party's case; or (iii) support another party's case. On the hearing of an application for an order under the above rules, the Court may dismiss or adjourn the application, if the Court is satisfied that discovery is not necessary, or not necessary at that stage of the cause or matter, if and so far as it is of the opinion that discovery is not necessary either for disposing fairly of the cause or matter or for saving costs.
4.	What are the general applicable laws and the scope in relation to takedown policies? (Related laws/regulations/directions/order and its applicability as well as domain name registration policies to takedown policies of IP rights)	In respect of copyright infringement, Section 43H of the CA provides that, if an electronic copy of a work accessible in a network infringes the copyright of the work, the copyright owner has the right to notify the service provider about the infringement. The service provider must comply within 48 hours from the receipt of the notification. Generally, under the CMA, the MCMC has in the past block access to offending or illegal websites based on complaints it receives as well as its ongoing surveillance. Under Section 211 of the CMA, no content applications service provider, or other person using a content applications service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten

		or harass any person. Further, it is an offence for a person who by means of any network facilities or network service or applications service knowingly makes, creates or solicits and initiates the transmission of, any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person; or initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address [Section 233 of the CMA]. MCMC may request for the assistance of any licensee under the CMA as far as reasonably necessary to prevent the commission or attempted commission of an offence under any written law of Malaysia or otherwise in enforcing the laws of Malaysia, including, but not limited to, the protection of the public revenue and preservation of national security [Section 262(2) of the CMA]. Further to the above, the CMA provides for the Communications & Multimedia Content Forum (**CMCF**) who is responsible for the preparation of a Content Code, or codes as the need may arise. The Malaysian Communications and Multimedia Content Code as of 14 February 2020 ("**Content Code**") issued by CMCF sets out the guidelines and procedures for good practice and standards of content disseminated to the audiences by services providers in the communications and multimedia industry in Malaysia. However, compliance with the Content Code is voluntary. Under Part 5 of the Content Code, if a code subject provides access to any content but neither control over the composition of the content or have any knowledge of such content is deemed an innocent carrier. An innocent carrier is not responsible for the content provided. Under the Content Code, take down procedures are clearly provided for. Internet Access Service Providers ("**IASP**") are required under Part 7.1 of the Code to incorporate terms and conditions in its contracts and legal notices and this includes terms that the IASP has right to block access or remove prohibited contents in accordance to any complaints filed under the Code. Once an IASP is notified by the Complaints Bereau that its users or subscribers are providing prohibited contents, the IASP, once identified the said user or subscriber, shall:- (i) Inform the subscriber to take down the prohibited content within 2 working days from the time of notification; (ii) Prescribe the period within which the prohibited content must be removed, ranging from 1 to 24 hours from the time of the notification;

		(iii) If the prohibited content is not removed, IASP shall be entitled to suspend or terminate the user or subscriber's access. Similar obligations are placed on Content Aggregators, Link Providers and Internet Content Hosting Providers. "Content Aggregator" means a person who aggregates and/or purchases Content; "Link Provider" means a person who provides links to other sites; "Internet Content Hosting Provider" means a provider in its capacity of merely providing access to content which is neither created nor aggregated by itself but which is hosted on its facilities. MYNIC (Malaysian Network Information Centre), the official domain name Registry in Malaysia is an agency under MCMC and governs the registration of domain names such as .my, .com.my, .org.my, .net.my, .edu.my, .gov.my, .mil.my and .name.my. MYNIC develops top-level domain name policies and dispute resolution policies. MYNIC has appointed the Asian International Arbitration Centre (AIAC) to facilitate .my domain name disputes. All domain name disputes are governed by MYNIC's Domain Name Dispute Resolution Policy (MYDRP), Sensitive Name Dispute Resolution Policy (SNDRP), Rules of the MYDRP and AIAC Supplementary Rules. MYDRP is the administrative procedure designed to provide simple, fast and affordable resolution of .my domain name disputes. If the complainant successfully prove that the disputed domain name is identical or similar to a trade or service mark of the complainant, and that the respondent registered and/or used the disputed domain name in bad faith, subject to the respondent proving its rights and legitimate interests in the disputed domain name, the registration of the disputed domain name will be transferred to the complainant or deleted. In addition to the above, SNDRP is the administrative process designed to govern complaints over use or registration domain names that contain a sensitive name. A sensitive name includes word or words in English, Malay or romanised Chinese (including dialects) and Indian dialects which:- (a) are sensitive to the Malaysian public; (b) are obscene, scandalous, indecent, offensive or contrary to Malaysian public norms or policy; (c) comprise of derivatives and colloquialisms of words that are offensive and/or (d) consist of pejorative expressions in terms of denotation, connotation or association.

		The registration of any domain name containing sensitive name will be deleted.
5.	What takedown obligations do the e-commerce sellers have? (Discussion on e-commerce sellers' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	Although Malaysian laws do not specifically provide for takedown obligations by e-commerce sellers, e-commerce sellers are generally subject to obligations to comply with laws and regulations governing consumer protection, payment, advertising, protection of intellectual property rights, and other relevant laws in respect of the sale of goods or services. In particular, the e-commerce sellers are required to comply with intellectual property laws whereby there may be liability for sale of counterfeit goods or goods or services riding on the intellectual property rights of third parties. Upon request or direction from the e-commerce platform and brand owners, e-commerce sellers would usually be required to remove the infringing materials. Particularly, by order of the Courts, sellers must take down such listings and/or any information prohibited by laws. Under the Content Code, e-commerce sellers may be considered as Content Aggregator and will therefore be subject to obligations of the same. If there are prohibited contents on its website, under Para 8.0 of the Content Code, the e-commerce sellers should take the following steps:- (i) Inform the subscriber to take down the prohibited content within 2 working days from the time of notification; (ii) Prescribe the period within which the prohibited content must be removed, ranging from 1 to 24 hours from the time of the notification; (iii) If the prohibited content is not removed, the Content Aggregator shall be entitled to remove the content.
6.	What takedown obligations do the platform operators have? (Discussion on the platform operators' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	Section 43H of the CA provides that, if an electronic copy of a work accessible in a network infringes the copyright of the work, the copyright owner has the right to notify the service provider about the infringement. The copyright owner must compensate the service provider against any damages, loss or liability arising from the compliance by the provider within 48 hours from the receipt of the notification. A service provider who has removed the infringing copy of the work shall notify the person who made available the infringing copy of the action taken by the service provider. The person whose work was removed or to which access has been disabled may send a counter-notice to the service provider. The service provider shall, upon receipt of the counternotice, promptly provide the issuer of the first notification with a copy of the counter-notice and inform the issuer that the removed work or access to the work will be restored in 10 business days, unless the service provider has received another notification from the issuer of the first notification informing it that he has filed an action seeking a court order to restrain the issuer of the counter

		notification from engaging in any infringing activity relating to the material on the service provider's network. Further, platform operators may be considered as Internet Content Hosting Provider. Under Para 10.1 of the Content Code, upon notification that its users or subscribers are providing prohibited content, the following steps should be taken:- (i) Inform the subscriber to take down the prohibited content within 2 working days from the time of notification; (ii) Prescribe the period within which the prohibited content must be removed, ranging from 1 to 24 hours from the time of the notification; (iii) If the prohibited content is not removed, the ICH shall be entitled to remove such content.
7.	Discussion on the takedown procedure i.e the procedures / steps.	As stated above under Section 43H of the CA, upon notification by the copyright owner, the service provider must comply within 48 hours from the receipt of the notification. A service provider who has removed the infringing copy of the work shall notify the person who made available the infringing copy of the action taken by the service provider. The person whose work was removed or to which access has been disabled may send a counter-notice to the service provider. The service provider shall, upon receipt of the counternotice, promptly provide the issuer of the first notification with a copy of the counter-notice and inform the issuer that the removed work or access to the work will be restored in 10 business days, unless the service provider has received another notification from the issuer of the first notification informing it that he has filed an action seeking a court order to restrain the issuer of the counter notification from engaging in any infringing activity relating to the material on the service provider's network.
8.	Are there any forthcoming changes to the law / regulations in relation to intermediary liability / takedown policies / practices?	Not for the time being.
9.	General comments on the current legal framework (Are there any interesting case studies or identified problems/issues).	There have been discussions between the Ministry of Domestic Trade and Consumer Affairs ("**MDTCA**") and the direct sales industry to clarify and review the applicability of the DSAPSA on e-commerce transactions and websites. Currently, under Section 19A of the DSAPSA, no person shall supply by sale, or advertise for the supply of, ***through electronic transaction***, any goods or services except in accordance with the DSAPSA or its regulations. "*sales through electronic transaction*" means sales of goods or services through electronic means by using **marketing networks** with the purpose of getting commission, bonus or any other economic advantage. "Marketing networks" are not however

		defined under the DSAPSA, although the ordinary usage of the phrase suggests that it involves a business model in which a distributor network is utilised. Nevertheless, since “marketing networks” are not statutorily defined, it is arguable that the phrase can also refer to a single-tier network. This has yet to be clarified by MDTCA.

Myanmar

Contributor: **Thomas Treutler** (Tilleke & Gibbins); **Ms. Yuwadee Thean-ngarm** (Tilleke & Gibbins Myanmar Limited)
Coordinator: Timothy Siaw (Shearn Delamore & Co.)

No.	Main Points	Answer
1.	Discussion on the general legal framework and scope of the laws governing e-commerce.	The Electronic Transactions Law (Law No. 5/2004), which was enacted on April 30, 2004, is an existing law relating to e-transaction matters. However, the law has no provisions specific to e-commerce transactions. There are some provisions in existing laws, such as the Telecommunication Law (Pyidaungsu Hluttaw Law No. 66/2013), Competition Law (Pyidaungsu Hluttaw Law No. 9/2015), and Consumer Protection Law (Pyidaungsu Hluttaw Law No. 9/2019), relating to advertising and promoting a product or commercial service by electronic means based on the type of activities. At present, substantive laws and regulations on e-commence businesses in Myanmar have yet to be enacted. The Ministry of Commerce's Department of Trade issued the **draft** Myanmar E-commerce Operation Guidelines 2020 (MEOG), but it has yet to be finalised. When implemented, this guideline will provide the essential legal framework on e-commerce businesses and transactions in Myanmar.
2.	What intermediary liabilities do the platform operators hold? (Discussion on the possible liabilities faced by platform operator i.e. contractual liabilities, personal data protection or intellectual property. Please include if there are any defences available for intermediaries.)	Based on the existing laws, platform operators hold the following intermediary liabilities in Myanmar: • must keep information transmitted or received through his service confidential and not disclose such information, except for matters allowed by the existing laws, of any individual user to any third person; • must not make advertisements with incorrect information of a product or service, thereby misleading consumers;

		• shall not carry out advertisements and broadcasts with false or misleading information to customers. There is no specific provision about defences available to intermediaries. If there is any administrative action for concerned prohibitions, an appeal may be petitioned to respective bodies according to the provisions of concerned laws and regulations. The draft MEOG provides the guidelines to be complied by a specified type of business: (i) to proceed the businesses in accordance with existing laws, regulations, and guidelines; (ii) to proceed in accordance with existing laws and regulations when requesting or using personal data of users or consumers; (iii) to avoid businesses infringing intellectual property rights under the Industrial Design Law, Trademark Law, Patent Law, and Copyright Law of Myanmar, which were enacted in 2019, and international agreements or treaties i.
3.	Whether brand owners have the right to request/demand for disclosure of the details of the alleged infringers (including, name, contact details, address, bank details) from the platform operators. (Discussion should include the relevant grounds for the request/demand, impact of personal data protection laws, the governing laws and regulations and the defences available for the platform operators)	Section 17 of the Telecommunication Law (Pyidaungsu Hluttaw Law No. 66/2013) states that "the licence holder shall keep the information transmitted or received through his telecommunication service confidential and shall not disclose such information of any individual user to any third person except for matters allowed by the existing laws." This provision suggests that platform operators cannot disclose details of alleged infringers, unless a concerned authority instructs a special condition in accordance with existing laws.
4.	What are the general applicable laws and the scope in relation to takedown policies? (Related laws/regulations/directions/order and its applicability to takedown policies of IP rights)	Myanmar enacted four IP laws (Industrial Design Law, Trademark Law, Patent Law, and Copyright Law) in 2019. All IP Laws are yet to be enforced, and subsequent rules, regulations, guidelines and policies relating to IP rights are expected to be tentatively issued and implemented next year.
5.	What takedown obligations do the e-commerce sellers have? (Discussion on e-commerce sellers' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	According to the existing laws and available information, e-commerce sellers are obliged to comply with the provisions including, but not limited to, advertising; marketing; promoting a product or services; prohibitions relating to intellectual property rights; and maintaining personal data of users,customers or consumers.

6.	What takedown obligations do the platform operators have? (Discussion on the platform operators' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	Under the current relevant laws and regulations, e-commerce sellers are obliged to comply with the provisions including, but not limited to, advertising; marketing; promoting a product or services; prohibitions relating to intellectual property rights; and maintaining personal data of users, customers or consumers.
7.	Discussion on the takedown procedure i.e. the procedures / steps.	Currently, there are no specific guidelines, laws and regulations providing the steps for taking action on the takedown procedure in Myanmar, except for actions related to criminal offences and breaches of morality etc.
8.	Are there any forthcoming changes to the law / regulations in relation to intermediary liability / takedown policies / practices?	For e-commerce transactions, the Ministry of Commerce is expected to issue the draft MEOG.
9.	General comments on the current legal framework (Are there any interesting case studies or identified problems/issues).	Notable case studies or identified problems/issues have not been officially reported because an e-commerce law has yet to be enacted. On the other hand, from our experience, we can report relevant case studies on Myanmar's current legal framework: for example, by sending cease-and-desist letters, we have successfully convinced persons selling counterfeit products on their Facebook pages and websites to remove such products.

New Zealand

Contributor: Kimberley Evans (Allens Patent & Trade Mark Attorneys)

No.	Main Points	Answer
1.	Discussion on the general legal framework and scope of the laws governing e-commerce	NZ law does not contain specific provisions that deal with intermediary liability in e-commerce, except by the *Copyright Act 1994* (NZ), which provides specific protections for internet service providers. Indirectly in relation to intermediary liability, the *Fair Trading Act 1986* (NZ) makes the following types of conduct illegal: • Deceptive or misleading conduct and false representations; • Unsubstantiated claims; • Unfair sales practices; and • Unfair contract terms. The Act applies to all commercial activities, trades, professions and businesses in New Zealand, as well as overseas businesses that supply goods, services or grant interests in land within New Zealand, including through online sales. Sellers cannot avoid their obligations under the Act by using an agent; agents are also bound by the provisions of the Act. However, e-commerce platform operators are unlikely to fall within the meaning of 'agent', which is likely to lead to difficulties in enforcing the provisions of the Act against e-commerce platform operators. The *Trade Marks Act 2002* (NZ) does not contain any provisions that specifically deal with intermediary liability. While the infringement provisions of the Act could potentially be utilised, it is likely that a trade mark owner would face difficulty showing that the online service provider or internet service provider has used the trade mark in a trade mark context.
2.	What intermediary liabilities do the platform operators hold? (Discussion on the possible liabilities faced by platform operator i.e. contractual liabilities, personal data protection or	The *Copyright Act 1994* (NZ) specifically provides for protections for internet service providers' (***ISP***) liability for material published online by a third party that infringes copyright. In summary, the protections are:

	intellectual property. Please include if there are any defences available for intermediaries.)	• Section 92B: Where a person uses the ISP's service while infringing copyright, the ISP, without more, does not infringe copyright, is not taken to have authorised the infringement and must not be subject to civil or criminal sanctions (though an injunction is allowed).
		• Section 92C: An ISP that stores a user's material that infringes copyright does not itself infringe the copyright, unless the ISP:
		  • Knows or has reason to believe the material infringes copyright; and
		  • Does not delete or prevent access to the material as soon as possible after becoming aware of it;
		  • Or – if the user of the ISP who provided the material is acting on behalf of or under direction of the ISP.
		• Section 92E: ISPs do not infringe copyright by caching material, except in limited circumstances.
		NZ commentators argue that these protections can be applied to most, if not all, parties that host user generated content, which could include e-commerce platform operators, depending on how the platform is constituted and operates.

3.	Whether brand owners have the right to request/demand for disclosure of the details of the alleged infringers (including, name, contact details, address, bank details) from the platform operators. (Discussion should include the relevant grounds for the request/demand, impact of personal data protection laws, the governing laws and regulations and the defences available for the platform operators)	Brand owners would need to obtain a court order under the *Trade Marks Act, Fair Trading Act* or *Copyright Act* in order to obtain details of infringers. E-commerce platform operators trading in NZ or to NZ consumers must have a privacy policy on their website, which governs the release of personal information to third parties. In addition, the *Privacy Act 1993* (NZ) limits the circumstances under which personal information can be disclosed, most of which require permission from the person to whom the data belongs or a court order.
4.	What are the general applicable laws and the scope in relation to takedown policies? (Related laws/regulations/directions/order and its	NZ has advanced legislation that forces platform operators to take down materials that threaten or harm individuals, promote terrorism or violent extremism. However, those

	applicability as well as domain name registration policies to takedown policies of IP rights)	provisions do not extend to intellectual property infringement. Brand owners would need to obtain a court order under the *Trade Marks Act, Fair Trading Act* or *Copyright Act* in order to obtain details of infringers. The *Copyright Act* also provides a three-notice process for copyright owners to take enforcement action against people who infringe copyright via file sharing. However, the process is strictly limited to infringement via file sharing. (See details at section 7 below.) Alternatively, brand owners may be able to have a domain name cancelled (or transferred to the brand owner) if the domain name is found to have been unfairly registered. A domain name is unfairly registered if it either: i) was registered or otherwise acquired in a manner which, at the time when the registration or acquisition took place, took unfair advantage of or was unfairly detrimental to the Complainant's Rights; OR ii) has been, or is likely to be, used in a manner which took unfair advantage of or was unfairly detrimental to the Complainant's Rights. This dispute process is administered by InternetNZ, which governs and manages the registration process for all .nz domain names. This is important because, if the commerce platform is not operated through a .nz domain name, the dispute process is not available.
5.	What takedown obligations do the e-commerce sellers have? (Discussion on e-commerce sellers' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	E-commerce sellers must comply with court orders requiring content to be taken down or modified.
6.	What takedown obligations do the platform operators have? (Discussion on the platform operators' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	Platform operators must comply with court orders requiring content to be taken down or modified.
7.	Discussion on the takedown procedure i.e the procedures / steps.	Specifically, and only, in relation to copyright infringement by file sharing, the following procedure applies: 1. The copyright owner gathers evidence and contacts the ISP, who can issue notices to the account holder. 2. The copyright owner contacts the ISP requesting that a Detection Notice be

		sent to the internet account holder and passes on the recorded internet protocol (IP) address associated with the computer or smart device that downloaded the infringing content. 3. The ISP matches the IP address to one of its customer accounts. The ISP is required by law to act on the owner's behalf, and where appropriate, issues infringement notices to the person who holds the identified account. (The ISP can charge for issuing notices, with the charges limited by the *Copyright Regulations*.) 4. The ISP can send up to three notices to the account holder for each alleged infringement: a Detection Notice, followed by a Warning Notice, and then the Enforcement Notice if file sharing activity continues. The Detection Notice includes information about the consequences of further infringing and how the account holder may challenge the notice. The account holder can cease the file sharing activity or challenge each notice. 5. The account holder can challenge a notice by completing a Challenge form accompanying the notice and send it back to their ISP. The ISP sends the Challenge form to the copyright owner, omitting the Account holder's name and contact details. 6. The copyright owner must respond to the ISP, otherwise the notice is cancelled. If the Challenge is accepted, the notice is cancelled and treated as if it wasn't issued; if rejected, the notice remains active. 7. The copyright owner can take a non-complying account holder to the Copyright Tribunal by filing the application, including a copy of the Enforcement Notice, any challenges, challenge responses, and the prescribed fee. Usually the Tribunal will make a decision based on the written submissions. Occasionally a hearing will be held at the request of the copyright owner, account holder,

		or the Tribunal itself. The Copyright Tribunal will issue its decision. The Tribunal has the ability to award damages to the copyright owner. The total amount cannot exceed NZ$15,000.
8.	Are there any forthcoming changes to the law / regulations in relation to intermediary liability / takedown policies / practices?	The NZ government is currently undertaking a review of the *Copyright Act* to ensure that the copyright regime remains fit for purpose in the context of a rapidly changing technological environment. In November 2019, the Ministry of Business, Innovation and Employment (***MBIE***) published a paper outlining revised objectives for copyright law in response to a public consultation that was conducted across 2018 and 2019. In response to stakeholder feedback, the MBIE withdrew that paper in July 2020. The next step in the review will be to publicly consult on potential changes to the objectives. There is no timeframe published on the MBIE's website for the proposed consultation.
9.	General comments on the current legal framework (Are there any interesting case studies or identified problems/issues).	N/A

Papua New Guinea

Contributor: **Kimberley Evans** (Allens Patent & Trade Mark Attorneys)

No.	Main Points	Answer
1.	Discussion on the general legal framework and scope of the laws governing e-commerce	Papua New Guinea contains a lot of rugged geography, which has resulted in limitations on the ability to develop infrastructure and internet connectivity. As a consequence, e-commerce in Papua New Guinea is quite limited and still in the process of developing as an industry. Since 2018, infrastructure developments have improved internet connectivity and reliability but internet access for the general population is still relatively limited. The Covid-19 pandemic has also been influential in the development and growth of online commerce as residents entered into lockdowns under state of emergency measures but e-commerce is not a dominant industry in PNG. As a result, Papua New Guinea does not have any legislation at this time that is specifically dedicated to the regulation of e-commerce. However, the following Acts contain provisions that can be applied to online use: ***Trade Marks Act 1978*** Under s53, a registered trade mark is infringed by a person who, not being the registered proprietor of the trade mark or a registered user of the trade mark using by way of permitted use, uses a mark which is substantially identical with, or deceptively similar to the trade mark, in the course of trade, in relation to goods in respect of which the trade mark is registered. The Court can order an injunction against an infringer. However, if the defendant establishes to the satisfaction of the Court that the use of the mark of which the plaintiff complains is not likely to deceive or cause confusion or to be taken as indicating a connection in the course of trade between the goods in respect of which the trade mark is registered and a person having the right, either as registered proprietor or as registered user, to use the trade mark, then an injunction cannot be granted.

		Copyright and Neighbouring Rights Act 2000 This Act prohibits the unauthorised reproduction of works in which copyright subsists, including literary, artistic and musical works. There is nothing within the Act that prevents the provisions being applied to online scenarios. Under s26, the Court has the power: (a) to grant injunctions to prohibit the committing, or continuation of committing, of an infringement of any right protected under this Act; or (b) to order the impounding of copies of works or sound recordings suspected of being made or imported without the authorization of the owner of any right protected under this Act where the making or importation of copies is subject to such authorization; or (c) to order the impounding or packaging of the implements that could be used for the making of copies of works and sound recordings, and the documents, accounts or business papers relating to such copies. ***Commerce (Trade Descriptions) Act 1952*** This Act was introduced in 1952 and is intended to be read in conjunction with the Customs Act 1951 (PNG). Because of its age, the provisions do not contemplate online use in their phrasing. However, it may be possible for trade mark owners to utilise the provisions of this Act to prevent misleading and deceptive conduct that takes place online. Under section 1 of this Act, "trade description", in relation to any goods, means a description, statement, indication, or suggestion, direct or indirect– (a) as to the nature, number, quantity, quality, purity, class, grade, measure, gauge, size or weight of the goods; or (b) as to the country or place in or at which the goods were made or produced; or (c) as to the manufacturer or producer of the goods or the person by whom they were selected, packed or prepared in any way for the market; or

		(d) as to the mode of manufacturing, producing, selecting, packing, or otherwise preparing the goods; or (e) as to the material or ingredients of which the goods are composed, or from which they are derived; or (f) as to the goods being the subject of an existing patent, privilege or copyright, and includes– (g) a Customs entry relating to the goods; and (h) and any mark that, according to the custom of the trade or common repute, is commonly taken to be an indication of any of the matters referred to in Paragraphs (a) to (f). Section 2(c) provides that a trade description will be deemed to be applied to goods if "it is used in any manner likely to lead to the belief that it describes or designates the goods", which arguably could be applied to online use and e-commerce. However, the Act would only apply where actual purchases are completed and the goods imported into PNG or exported out of PNG. Sanctions under the Act include fines and forfeiture of the goods, but do not extend to injunctions or take down notices. ***Commercial Advertisement (Protection of the Public) Act 1976*** The purpose of the Act is to protect the general public from any commercial advertisement containing untrue, inaccurate, misleading, misrepresentative or unreasonable statements used when describing the size, quality, quantity, or nature of goods or services. However, the definition of "advertisement" in the Act limits the application of the Act to advertisements (any invitation to purchase or use the goods/services) that are specifically sent to or directed at particular persons inside PNG. In other words, advertisements that are intended for the world at large (and not just PNG consumers) but may be seen by PNG residents will not fall within the scope of the Act. It is likely that any protection afforded to trade mark owners under the Act would be very limited and unlikely to apply to any global e-

		commerce platforms unless the platform directly targets PNG individuals. Sanctions under the Act are limited to fines and correction of the unfair statement.
2.	What intermediary liabilities do the platform operators hold? (Discussion on the possible liabilities faced by platform operator i.e. contractual liabilities, personal data protection or intellectual property. Please include if there are any defences available for intermediaries.)	PNG law does not specifically address the issue of intermediary liability.
3.	Whether brand owners have the right to request/demand for disclosure of the details of the alleged infringers (including, name, contact details, address, bank details) from the platform operators. (Discussion should include the relevant grounds for the request/demand, impact of personal data protection laws, the governing laws and regulations and the defences available for the platform operators)	PNG law does not specifically address this issue. Privacy laws in PNG only extend to private communications, not communications for the purpose of commerce (see the *Protection of Private Communications Act 1986*).
4.	What are the general applicable laws and the scope in relation to takedown policies? (Related laws/regulations/directions/order and its applicability as well as domain name registration policies to takedown policies of IP rights)	Aside from the laws governing the protection of intellectual property rights and the prohibition of misleading commercial activities which may apply to e-commerce situations, PNG law does not address this issue. From a domain name perspective, the .pg domain name registration policy requires registrants to warrant that they have the right to use and register the domain name and also that the use and registration does not interfere with or infringe the intellectual property rights of any 3rd party. The exclusive .pg domain name registrar, PNG University of Technology, has the discretion to refuse a request to register a domain name. The PNG University of Technology will also withdraw a .pg domain name from use and registration if ordered by a PNG court that the domain name rightfully belongs to another party.
5.	What takedown obligations do the e-commerce sellers have? (Discussion on e-commerce sellers' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	PNG law does not address this issue. However, e-commerce sellers would be bound by the terms and conditions of any e-commerce platform from which they operate.
6.	What takedown obligations do the platform operators have? (Discussion on the platform operators' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	IP rights holders would need to obtain an injunction from the court in order to have an enforceable takedown order. However, there is no case law in PNG on takedown orders.

7.	Discussion on the takedown procedure i.e the procedures / steps.	n/a
8.	Are there any forthcoming changes to the law / regulations in relation to intermediary liability / takedown policies / practices?	On 1 June 2020, the National Executive Council approved the introduction of the *Electronic Transactions Bill* into Parliament. The purpose of the Bill is to enable a legal framework for the use of electronic transactions and will address a number of issues, including: • Promoting the development of the legal and business infrastructure necessary to implement secure electronic commerce; and • Promoting public confidence in the integrity and reliability of electronic commerce. The Bill is intended to have broad scope and will apply to any kind of data message, electronic document or other information used in the context of commercial activities, including domestic and international dealings, transactions, arrangements, agreements, exchanges and storage of information. It is expected that this Bill will begin to establish a regulatory framework for e-commerce in PNG.
9.	General comments on the current legal framework (Are there any interesting case studies or identified problems/issues).	Law in relation to e-commerce in PNG is still developing so it is expected that there will be significant developments within the next few years.

South Korea

Contributor: S. Yong Lee (Y.P. Lee,Mock & Partners)
Coordinator: Yunze LIAN of Jadong IP Law Firm

No.	Main Points	Answer
1.	Discussion on the general legal framework and scope of the laws governing e-commerce	In Korea, there are the following two laws governing e-commerce: - Act on the Consumer Protection in Electronic Commerce, etc. - Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. The relevant provisions of each law which may be related to the intermediary liability of the platform operator are as follows: **Act on the Consumer Protection in Electronic Commerce, etc.** Article 2 (Definition) 1. The term “electronic commerce transaction" means conducting commercial activities by means of an electronic transaction; 2. The term "mail order" means selling goods or services by providing information on the sale of goods, etc. and receiving a consumer's order by means of mail, telecommunications or other methods prescribed by Ordinance of the Prime Minister; 3. The term "mail order distributor" means a person who is engaged in mail order or a person who conducts the mail order business in accordance with a contract with the former; 4. The term "mail order brokerage" means the act of intermediating a mail order between both parties to a transaction by allowing the use of a cybermall (referring to a virtual shopping mall established to transact goods, etc. using computers, etc. and information communications facilities; hereinafter the same shall apply), or by other methods prescribed by Ordinance of the Prime Minister; Article 20 (Obligations and Liabilities of Mail Order Brokers) (2) If a person who has requested mail order brokerage is a business operator, a person

		who conducts the brokerage of mail orders as a business who is a mail order distributor shall confirm the name, address, telephone number and other matters prescribed by Presidential Decree, and provide them to consumers before the conclusion of an order, and if a requester of mail order brokerage is not a business operator, a mail order broker who is a mail order distributor shall confirm the name, telephone number and other matters prescribed by Presidential Decree and provide both parties to the transaction with the method to access the information on the other party. (3) In order to resolve complaints or disputes arising from the use of cybermalls, etc., a mail order broker shall find out the cause thereof, assess damage and take other necessary measures without delay. Article 20-2 (Liability of Mail Order Brokers and Requesters of Mail Order Brokerage) (2) A mail order broker shall be jointly liable with the requester of mail order brokerage for the damage caused to the consumer's property by failing to provide information or a method to access information under Article20 (2), or by providing false information: Provided, That this shall not apply where he/she has paid due attention to prevent any damage to the consumers **Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.** Article 44 (Protection of Rights in Information and Communications Networks) (1) No user may circulate any information violative of other person's rights, including invasion of privacy and defamation, through an information and communications network. (2)Every provider of information and communications services shall make efforts to prevent any information under paragraph (1) from being circulated through the information and communications network operated and managed by the provider. (3) The Korea Communications Commission may prepare a policy on technological development, education, public relations activities, and other activities to prevent violation of other persons' rights by information circulated through information and communications networks, including invasion

		of privacy and defamation and may recommend providers of information and communications services to adopt the policy. Article 44-2 (Request for Deletion of Information) (1) Where information provided through an information and communications network purposely to be made public intrudes on other persons' privacy, defames other persons, or violates other persons' right otherwise, the victim of such violation may request the provider of information and communications services who managed the information to delete the information or publish a rebuttable statement presenting explanatory materials supporting the alleged violation. (2) Upon receiving a request for deletion or rebuttal of the information under paragraph (1), a provider of information and communications services shall delete the information or take a temporary or any other necessary measure and shall notify the applicant and the publisher of the information immediately. (4) Notwithstanding a request for deletion of the information under paragraph (1), if it is impracticable to judge whether information violates any right or it is anticipated that there will probably be a dispute between interested parties, a provider of information and communications services may take a measure to block access to the information temporarily. In such cases, the period for the temporary measure shall not exceed 30 days. (5) Every provider of information and communications services shall clearly state in advance the details, procedures, and other matters regarding necessary measures in the terms and conditions. (6) If a provider of information and communications services takes necessary measures under paragraph (2) for the information circulated through the information and communications network operated and managed by himself or herself, the provider may have his or her liability to indemnify loss incurred by such information mitigated or discharged.
2.	What intermediary liabilities do the platform operators hold? (Discussion on the possible liabilities faced by platform operator i.e. contractual liabilities, personal data protection	In Korea, there is no special law defining the intermediary liabilities of the platform operators. Also, Korean Trademark Act does

	or intellectual property. Please include if there are any defences available for intermediaries.)	not have a provision of liabilitiesto contributory infringement against a trademark right. Especially, the Supreme Court held that "any information that infringes upon other's rights through invasion of privacy, defamation, etc." under Article 44 (2) of Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.does not include information infringing upon other's trademarks and therefore the provision cannot be construed to impose alleged duty on service providers. (Case No. 2010 Ma 817) Further, the Supreme Court found that the platform operators are not automatically liable for the sale of infringing products, as they are not actively engaged in the infringing activities. In this regard, the court provided the following requirements to consider when determining whether the platform operator is liable for contributory infringement against a trademark right: 1) whether the products sold in the platform infringe; 2) whether the trademark owners have made specific requests to prevent sales of the infringing products, and that the platform operator would have been aware of the infringing products; and 3) whether the platform operator failed to act to prevent such sales, notwithstanding its ability to do so. On the contrary, the platform operators should bear intermediary liabilities if they do not take proper measures preventing the infringing activities from being stopped even when all of the above-referenced three requirements are met. In this regard, the intermediary liabilities of the platform operators are based on the following provisions of Korean Civil Act: **Civil Act** Article 760 (Liability of Joint Tort-feasors) (3) Instigators and accessories shall be deemed to act jointly. Furthermore, relevant provisions of Trademark Act, and Unfair Competition and Prevention and Trade Secret Protection Act would be the basis of the trademark protection as well.
3.	Whether brand owners have the right to request/demand for disclosure of the details of	According to the Supreme Court, however, the platform operators are not required to provide

	the alleged infringers (including, name, contact details, address, bank details) from the platform operators. (Discussion should include the relevant grounds for the request/demand, impact of personal data protection laws, the governing laws and regulations and the defences available for the platform operators)	information about the seller of the infringing products to the trademark owner. (Case No. 2010 Ma 817) Meanwhile, according to Article 20 (2) of Act on the Consumer Protection in Electronic Commerce, etc., the platform operators should provide the name, address, telephone number, business license number, email address and information on credit about a mail order broker on the platform to consumers. Therefore, brand owners may easily recognize the general information of the mail order broker from the platform.
4.	What are the general applicable laws and the scope in relation to takedown policies? (Related laws/regulations/directions/order and its applicability as well as domain name registration policies to takedown policies of IP rights)	Article 44-2 of Act on Promotion of Information and Communications Network Utilization and Information Protection, etc, is an on-demand takedown provision. As we reviewed from Case No. 2010 Ma 817 of the Supreme Court, however, this provision applies only to "any information that infringes upon other's rights through invasion of privacy, defamation, etc.", and the information infringing upon other's trademarks do not belong to "any information that infringes upon other's rights through invasion of privacy, defamation, etc." Therefore, takedown policies of IP rights cannot be based on Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. However, the platform operators should take proper measures preventing the infringing activities from being stopped on their platform when brand owners indicate an apparent goods of trademark infringement on the platforms and request a proper measure like a takedown from the platforms. Otherwise, the platform should bear intermediary liabilities based on Article 760 (3) Liability of Joint Tort-feasors of Civil Act, together with relevant provisions of Trademark Act.
5.	What takedown obligations do the e-commerce sellers have? (Discussion on e-commerce sellers' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	Basically, the e-commerce sellers take responsibilities for infringements against IP rights such as damage compensation, recovery of reputation, etc. based on Trademark Act, Patent Act, Design Protection Act and Copyright Act. Absolutely, these responsibilities include takedown obligations and other liabilities preventing the IP infringements activities from being stopped. Further, the platform operators generally request the e-commerce sellers to follow

		contractual terms and conditions for using the platform. In this regard, the platform operators insert duties of not infringing IP rights of others, acquiring permission from IP right owners when using a brand, image, or any IP assets, etc. into the contractual terms and conditions.
6.	What takedown obligations do the platform operators have? (Discussion on the platform operators' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	According to Article 20 (3) (Obligations and Liabilities of Mail Order Brokers) of Act on the Consumer Protection in Electronic Commerce, etc., the platform operators should take a necessary measures without delay when complaints or disputes arise from the platform. In this regard, the necessary measures may include a takedown. Also, the platform operators may request e-commerce sellers to follow contractual terms and conditions for using the platform such as to not infringe IP rights of others, stop selling of goods infringing IP rights of others until a court decision will be issued, etc.
7.	Discussion on the takedown procedure i.e the procedures / steps.	Generally, the takedown procedures on the platforms consist of the following steps: - Request or application of IP owners for a takedown with evidences - Forwarding of the request or application by the platform operators to the e-commerce sellers - Answering of the e-commerce sellers to the platform operators - Certain process of the platform operators for judgement - Acceptance or rejection of the request or application for the takedown
8.	Are there any forthcoming changes to the law / regulations in relation to intermediary liability / takedown policies / practices?	In Korea, there has been a discussion for adopting provisions such as limitation on liability as well as intermediary liabilities of the platform operators in Trademark Act. However, such an amendment of Trademark Act has not yet concluded.
9.	General comments on the current legal framework (Are there any interesting case studies or identified problems/issues).	On the one hand, it is useful for protection of trademark to establish intermediary liabilities of the platform operators in Trademark Act. On the other hand, excessive intermediary liabilities to the platform operators may hinder e-commerce developments. In this regard, it would be very valuable to continuously make an effort for finding a balance between trademark protection and e-commerce

		developments. Further, it may be one of solutions to find a way of cost reduction for checking trademark infringements on platform based on technology of digitalization and security or equivalents thereof.

Thailand

Contributor: **Priyanka Vedak** (Reliance Industries Limited)

No.	Main Points	Answer
1.	Discussion on the general legal framework and scope of the laws governing e-commerce	Thailand has a sui generis law dealing particularly with E-Commerce which are a. Electronic Transactions Act (2001) – The Act recognizes that online transaction is valid, but contains no specific provision dealing with consumer protection. b. Computer Crime Act (2007) - The CCA ultimately acts as a consumer-protection mechanism and as a signal to the greater market that the Thai e-commerce platform is safe, secured, and effectively monitored by the state apparatus. c. Payment System Act (2017) - The Payment System Act (PSA) is arguably the most dynamic of recent Thai legislation in the e-commerce arena. It aims to synthesize existing payment regulations while synchronizing them with international standards. It also allows structural flexibility to regulate any new payment systems that may emerge in the future. d. Personal Data Protection Bill - Unlike the stringent consumer protections offered by the GDPR, there is no analogous data protection legislation in Thailand.
2.	What intermediary liabilities do the platform operators hold? (Discussion on the possible liabilities faced by platform operator i.e. contractual liabilities, personal data protection or intellectual property. Please include if there are any defences available for intermediaries.)	Combined with Questioner 1
3.	Whether brand owners have the right to request/demand for disclosure of the details of the alleged infringers (including, name, contact details, address, bank details) from the platform operators. (Discussion should include the relevant grounds for the request/demand, impact of personal data protection laws, the	

	governing laws and regulations and the defences available for the platform operators)	
4.	What are the general applicable laws and the scope in relation to takedown policies? (Related laws/regulations/directions/order and its applicability as well as domain name registration policies to takedown policies of IP rights)	**Copyright Act** 1. The amended Thai Copyright Act (No. 2), which came into force on August 4, 2015, provides copyright owners with a tool to tackle online infringement. Section 32/3 allows for preliminary injunctions that remove copyright-infringing works from the internet, while at the same time providing an exemption from liability for internet service providers (ISPs). Under this section, the copyright owner must file a motion with the court requesting an injunction order against the infringing material. The motion must clearly state any information regarding the ISP, infringement claims, and details of the investigation process that will lead to the finding of the infringement and evidence thereof, including the potential damages and other relevant factors. If all required information is provided and the court sees the necessity, the court may order the ISP to remove the copyright-infringing content. Afterwards, the copyright owner must initiate legal action against the actual infringer within a specified time period. *Obstacles* However, copyright owners have had some issues in getting injunctions under this section. In many of the unsuccessful cases, the court rejected the grant of injunctive relief because copyright owners had, in the court's view, failed to provide sufficient information, such as details and evidence of the investigation process. Even if the court grants an injunction order, there are still obstacles in the implementation process. Takedown orders targeting foreign ISPs with servers hosted outside of Thailand are often unenforceable since Section

		32/3 does not explicitly provide for website blocking. As a result, some copyright owners have turned their focus to other enforcement options. **Computer Crime Act** Prior to the amendment of the Computer Crime Act (CCA), there was an idea to apply Sections 14(1) and 20 of the old Computer Crime Act B.E. 2550 (2007) to address IP infringement on the internet. The old CCA provided a mechanism for a government officer to ask the court to block the distribution of forged computer data or false computer data, which were contrary to the public order or good morals. But this approach was not feasible in practice because it was hard to define the act of offering counterfeit goods for sale, or the sharing of pirated movies by internet users, as distributing "forged computer data" or "false computer data." Thus, officials have been reluctant to take action against these types of IP infringement offenses on the Internet. *Section 20(3) of the Amended Computer Crime Act* Recently, the CCA was amended to solve several issues, including adding new enforcement measures to tackle online IP infringement. The Computer Crime Act (No. 2) B.E. 2560 (2017), which takes effect on May 24, 2017, provides a permanent injunction to block websites that have online IP-infringing content or for removing such data. Section 20(3) states that where there is dissemination of computer data which is a criminal offense against intellectual property, an official may, with approval from the Minister of Digital Economy and Society, file a motion with evidence to the court requesting the cessation of dissemination or deletion of such computer data from the computer system. Under the CCA the Ministry of Digital Economy and Society (MDES), and its officials have primary authority related to these provisions. *Implementing the Procedure* In practice, it is usually the IP owner who finds the alleged infringement on a website. The IP owner may provide the URL of the website to

		an officer of the MDES assigned to investigate and collect evidence for further consideration by the Minister. Once the Minister approves, the officer will then file a motion with the court requesting that the website be blocked or its content deleted. However, in an urgent case, the officer may file a motion with the court before obtaining approval from the Ministry. If this is the case, the officer must report the matter to the Minister as soon as possible after the motion has been filed. Finally, if the court grants the request, the officer may either block the website or order the ISP to do so. The rules, timeline, and methods for enforcing the court order are regulated by the Minister's Notification.
	What takedown obligations do the e-commerce sellers have? (Discussion on e-commerce sellers' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	N/A
	What takedown obligations do the platform operators have? (Discussion on the platform operators' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	N/A
5.	Discussion on the takedown procedure i.e the procedures / steps.	The process/steps for the Ecommerce platforms are 1. The E-commerce Platform investigates the formality of the claim; 2. The alleged infringer will be notied by the Ecommerce Platform; 3. The alleged infringer can submit a counternotification proving authorisation of sales; 4. The IP-owner can either accept the counternotification or submit the case for dispute; 5. Claims will be handled through the E-commerce platform: a standardised programme through which IP owners

		can notify ownership prior to online advertising
6.	Are there any forthcoming changes to the law / regulations in relation to intermediary liability / takedown policies / practices?	N/A
7.	General comments on the current legal framework (Are there any interesting case studies or identified problems/issues).	N/A

Taiwan

Contributor: Benjamin Y. Li (Lee and Li, Attorneys at law); Wei-Ting Liao (Lee and Li, Attorneys at law)[2]
Coordinator: Julia Hongbo ZHONG (Lee and Li – Leaven IPR Agency Ltd.)

No.	Main Points	Answer
1.	Discussion on the general legal framework and scope of the laws governing e-commerce	The legal framework of the laws governing e-commerce in Taiwan includes the Civil Code, the Personal Data Protection Act and the Copyright Act. The Trademark Act and the Patent Act do not provide specific articles governing liability of intermediaries and the takedown policies/practices; however, the platform operator may still face liability of trademark or patent infringement on a case-by-case basis.
2.	What intermediary liabilities do the platform operators hold? (Discussion on the possible liabilities faced by platform operator i.e. contractual liabilities, personal data protection or intellectual property. Please include if there are any defences available for intermediaries.)	According to the above acts and codes (namely Civil Code, the Personal Data Protection Act, the Copyright Act, the Trademark Act and the Patent Act), the platform operator may hold contractual liabilities, liability of infringement, liabilities of failure of personal data protection and liability of intellectual property infringement. To alleviate the risk of infringement liabilities (especially intellectual property infringement), the platform operator may exempt his liabilities via contractual design. An "Internet service provider" ("ISP") could be exempted from civil liabilities of infringement if the ISP is entitled to the safe harbour regime according to Article 90-4 of the Copyright Act.
3.	Whether brand owners have the right to request/demand for disclosure of the details of the alleged infringers (including, name, contact details, address, bank details) from the platform operators. (Discussion should include the relevant grounds for the request/demand, impact of personal data protection laws, the governing laws and regulations and the defences available for the platform operators)	The brand owners do not have the right to request/demand for disclosure of the details of the alleged infringers. According to Article 20 of the Personal Data Protection Act, a non-government agency shall use general personal data only within the necessary scope of the specific purpose of collection; the use of personal data for another purpose shall be only based on one of the following conditions:

[2] The information provided herein is a general overview of Taiwan's regulatory regime on the specific topic, and is not intended to be a comprehensive review of all related issues or developments nor should it be taken as an opinion or legal advice on the matters covered.

		1. where it is expressly required by law; 2. where it is necessary for furthering public interests; 3. where it is to prevent harm on life, body, freedom, or property of the data subject; 4. where it is to prevent material harm on the rights and interests of others; 5. where it is necessary for statistics gathering or academic research by a government agency or an academic institution for public interests; provided that such data, as provided by the data provider or disclosed by the data collector, may not lead to the identification of a specific data subject; 6. where consent has been given by the data subject; or 7. where it is for the data subject's rights and interests.
4.	What are the general applicable laws and the scope in relation to takedown policies? (Related laws/regulations/directions/order and its applicability as well as domain name registration policies to takedown policies of IP rights)	Articles 90-4 to 90-12 of the Copyright Act govern the safe harbour regime for the platform operators. According to Article 90-7 of the Copyright Act, the copyright owner and the plate right owner could initiate the takedown process by notifying the platform operators. Article 3, Paragraph 1 of the *"Regulations Governing Implementation of ISP Civil Liability Exemption" (hereinafter "the Regulations")* provides that the notification of the rights owner shall specify the particulars listed below: 1. The name, address, and telephone number or fax number or electronic mail address or description of other automatic communication of the rights holder or agent thereof. 2. The name of the copyrights or plate rights infringed. 3. A statement requesting the removal of, or disabling of access to, the content that allegedly infringes copyright or plate rights. 4. Access or relevant information sufficient to enable the Internet service

		provider to identify the allegedly infringing content. 5. A statement that the rights holder or the agent thereof is acting in good faith and in the belief that the allegedly infringing content lacks lawful licensing or is otherwise in violation of the Copyright Act. 6. A declaration that the rights holder is willing to bear legal liability in the event there is misrepresentation with resultant injury to another.
5.	What takedown obligations do the e-commerce sellers have? (Discussion on e-commerce sellers' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	Articles 90-4 to 90-12 of the Copyright Act do not impose any takedown obligation on the e-commerce sellers. The Copyright Act only imposes takedown obligations on the platform operators.
6.	What takedown obligations do the platform operators have? (Discussion on the platform operators' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	Pursuant to Article 90-7 of the Copyright Act, a platform operator, who is an "ISSP" (Information Storage Service Provider: those who provide information storage services at the request of a user through a system or network controlled or operated by the service provider), may be exempt from the liabilities for infringement of the copyright or plate rights of another by a user of its service if the ISSP: 1. does not have knowledge of the allegedly infringing activity of the user; 2. does not receive a financial benefit directly attributable to the infringing activity of the user; and 3. **responds expeditiously to remove, or disable access to, the allegedly infringing content or related information upon notification by a copyright holder of the alleged infringement by the user of the ISSP**. Pursuant to Article 90-9 of the Copyright Act, when ISSP removes the allegedly infringing content or related information, **ISSP should proceed with the following actions**: 1. notify the allegedly infringing user of such removal or disconnection. 2. such user may request the ISSP to restore the removed content or the access to it (i.e. a counter notification).

		3. an ISSP shall further notify the copyright holder of the user's counter notification. 4. if, within 10 business days after receiving counter notification from the ISSP, the copyright holder provides the ISSP with the evidence regarding filing civil or criminal litigation against the user, the ISSP shall not bear any obligation to restore the content or related information. However, if the copyright holder fails to provide such evidence, the ISSP shall restore the removed content or the access to it within 14 business days from the next day of further notification of the user's counter notification.
7.	Discussion on the takedown procedure i.e. the procedures / steps.	Provided in Row 6 of this Table.
8.	Are there any forthcoming changes to the law / regulations in relation to intermediary liability / takedown policies / practices?	The Bill of Digital Communications Act provides intermediary liability, exemption of intermediary liability and takedown policies.
9.	General comments on the current legal framework (Are there any interesting case studies or identified problems/issues).	Liability of intermediaries and the takedown policies/practices are mainly provided in the Copyright Act. The contractual liabilities, liability of infringement and liability of trademark/patent infringement are determined on a case-by-case basis. Recently, a judgment of the Intellectual Property Court (ongoing case) decided that the platform operator is liable to trademark infringement since the platform operator's extent of involvement to the transaction is higher than a general platform operator.

Uzbekistan

Contributor: Djakhangir Aripov (PETOSEVIC Uzbekistan)

No.	Main Points	Answer
1.	Discussion on the general legal framework and scope of the laws governing e-commerce	The following laws and regulations are applicable in Uzbekistan in the field of intermediary liability and takedown policies in respect of trademark infringements: The Law of the Republic of Uzbekistan on "ELECTRONIC COMMERCE" (new edition) No. 385, dated on May 22, 2015, constitutes general legal framework of the e-commerce laws in Uzbekistan. The Rules of e-commerce, approved by the Cabinet of Ministers of the Republic of Uzbekistan from June 2, 2016 № 185 set out general rules. The Law of the Republic of Uzbekistan on "TELECOMMUNICATIONS" No. 822 – I, dated on August 20, 1999 emphasize on operator duties and obligations as well as their liabilities. The details are discussed below.
2.	What intermediary liabilities do the platform operators hold? (Discussion on the possible liabilities faced by platform operator i.e. contractual liabilities, personal data protection or intellectual property. Please include if there are any defences available for intermediaries.)	**Article 13** of the Law of Republic of Uzbekistan on "ELECTRONIC COMMERCE" No. 385 highlights rights and obligations of information intermediaries. An information intermediary is not responsible for legal consequences related to the content of electronic documents and electronic communications of e-commerce transmitted by the participants. The information intermediary may have other rights and bear other obligations in accordance with the legislation and the contract. **Paragraph 19** of the Rules of e-commerce, approved by the Cabinet of Ministers of the Republic of Uzbekistan from June 2, 2016 № 185 highlight that an information intermediary is not obliged to control or verify the authenticity of transmitted, received, and stored electronic documents as well as electronic messages, and their compliance with the law, unless otherwise provided by law or contract.

		Article 21 of the Law of the Republic of Uzbekistan on “TELECOMMUNICATIONS” No. 822 – I states that operators and providers shall have the right: to suspend provision of services to users in case of violation of the established rules on use of telecommunications; to reimburse losses incurred through the fault of legal entities and individuals; to appeal against illegal actions of legal entities and individuals in accordance with the legislation. While **Article 22** of the abovementioned Law emphasizes that operators and providers should indemnify users for improper performance of telecommunication services contracts, as well as in accordance with the law. **Article 64** of the amended version of the Law of the Republic of Uzbekistan "On copyright and related rights", July 20, 2006, toughens responsibility for violation of authors' rights in Uzbekistan. This toughening applies to Internet providers. The adopted Law contains the term "making available to the public". This action represents the exclusive right of the authors. However, with regard to Trademarks, there is a loophole in legislation as liability of intermediaries on e-commerce is not addressed properly, thus, it remains quite ambiguous. For this reason, **Civil Code, Article 1107** “Responsibility for Violation of the Right to the Trademark” should apply. The person who uses the trademark illegally is obliged to stop the infringement and compensate the trademark owner for the losses incurred. The person who uses the trademark illegally is obliged to destroy the produced images of the trademark, remove the illegally used trademark or a designation similar to it to the degree of confusion from the goods or its packaging. If it is impossible to fulfill the requirements set forth in point two of this Article, the goods in question shall be subject to destruction. Applicability of the abovementioned legal norms to intermediaries however, is not clear, most probably they could only be liable if properly informed about the infringement and there is no information about the actual infringer who could

		be sued before the court. Intermediaries can be involved as co-defendants in a trademark infringement lawsuit if they have been priorly informed about the violation and no action was taken by them to take down the infringement.
3.	Whether brand owners have the right to request/demand for disclosure of the details of the alleged infringers (including, name, contact details, address, bank details) from the platform operators. (Discussion should include the relevant grounds for the request/demand, impact of personal data protection laws, the governing laws and regulations and the defences available for the platform operators)	**Article 18** of the Law of the Republic of Uzbekistan on "ELECTRONIC COMMERCE" No. 385 ensures that in e-commerce the use of personal data for purposes other than the purposes of the contract in electronic commerce is forbidden as well as their transfer to third parties, unless otherwise agreed by the parties' agreement and/or legislation. It is forbidden to use personal data without the consent of their owner for the distribution of an offer and/or advertising, including such means as mass mailing of electronic documents or electronic messages. **Article 12** of the Law "On personal data" stresses that the use of personal data by the employees of the owner and/or operator, as well as of the third party, connected with the processing of personal data, should be carried out only in accordance with their professional, official or labour duties. The employees of the owner and/or operator, as well as of the third party, connected with the personal data processing, are obliged to prevent the disclosure of personal data that were entrusted to them or became known to them in connection with their professional, official or labour duties. **Article 13** on providing personal data states that The provision of personal data to the public administration authorities is performed free of charge. The subject, when refusing to provide his personal data, has the right not to indicate the reasons for his refusal. Finally, **article 28** on confidentiality of personal data provides that the owner and/or operator and other persons who have gained access to personal data are obliged not to disclose and distribute personal data without the consent of the subject. Thus, it is unlikely that the brand owners can gain personal data of the infringers without getting consent of the latter or the court order.

		Criminal Code, **article 143** violation of the confidentiality of correspondence, telephone conversations, telegraphic or other messages committed after the application of administrative penalty for the same actions - shall be punishable by a fine of up to twenty-five basic units of account or by deprivation of a certain right for up to three years, or by compulsory community service for up to three hundred and sixty hours, or by corrective work for up to three years. In our experience, personal data can only be disclosed to the right holder by the court's order addressed to the intermediary. This is usually very unlikely to achieve, which makes it very difficult to enforce trademark rights against natural persons owning domain names in the .UZ cctld.
4.	What are the general applicable laws and the scope in relation to takedown policies? (Related laws/regulations/directions/order and its applicability as well as domain name registration policies to takedown policies of IP rights)	**Civil Code, Article 1107** "Responsibility for Violation of the Right to the Trademark" should apply. The person who illegally uses the trademark is obliged to stop the infringement and compensate the trademark owner for the losses incurred. The person who illegally uses the trademark is obliged to destroy the produced images of the trademark, remove the illegally used trademark or a designation similar to it to the degree of confusion from the goods or its packaging. If it is impossible to fulfill the requirements set forth in point two of this Article, the goods in question shall be subject to destruction. **Administrative Code, Article 177** "Illegal use of someone else's trademark, service mark, appellation of origin of goods or firm's name" Illegal use of someone else's trademark, service mark, appellation of origin of goods or similar to the extent of confusion of designations for homogeneous goods (services) or illegal use of someone else's trade name - imposes a fine on citizens from five to ten, and on officials - from ten to twenty basic calculated values. The same offences committed again within a year after the application of the administrative penalty, -

		shall be punishable by a fine of ten to twenty for citizens and twenty to thirty basic calculation units for officials. **Civil Code, Article 1107** "Responsibility for Violation of the Right to the Trademark" should apply. The person who uses the trademark illegally is obliged to stop the infringement and compensate the trademark owner for the losses incurred. The person who uses the trademark illegally is obliged to destroy the produced images of the trademark, remove the illegally used trademark or a designation similar to it to the degree of confusion from the goods or its packaging. All IPR violations in the field of domain names in the .UZ cctld can be usually be resolved through negotiations with the adverse party, by filing an unfair competition action (enforceable through the court only) or the court.
5.	What takedown obligations do the e-commerce sellers have? (Discussion on e-commerce sellers' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	According to the Rules of e-commerce, approved by the Cabinet of Ministers of the Republic of Uzbekistan from June 2, 2016 № 185's duties, **article 11,** the seller must: - comply with competition and consumer protection legislation in the sale of goods (works, services) in electronic commerce, including providing the buyer necessary and reliable information about the goods (works, services); - ensure the proper storage of electronic documents and electronic communications; - provide other participants of e-commerce with appropriate access to reliable information about themselves in electronic form in the state language and, if necessary, in other languages, which should include the following information: full name of the entrepreneur with indication of its legal form - for a legal entity; name, surname, patronymic - for an individual engaged in entrepreneurial activity without formation of a legal entity; information on state registration, taxpayer identification number of the entrepreneur; location (postal address), e-mail address, contact phone number; in cases stipulated by the legislation - information on the availability of a license or a

		permit (number of a license or a permit document, validity period, name of the body authorized to issue a license or a permit document). - an offer or information about goods (works, services) offered by the seller must be submitted in electronic form, which allows to reproduce the information without any distortion and make a reliable idea about the seller, as well as about the goods (works, services) offered by the seller, prices and tariffs on them, as well as the conditions of their sale (performance of works, provision of services). **Article 20** of the Law of the Republic of Uzbekistan on “TELECOMMUNICATIONS” No. 822 – I Elimination of consequences of accidents on telecommunication networks states that the losses caused to the owner as a result of liquidation of consequences of incidents are subject to compensation by the corresponding operator. Losses caused to operators and providers as a result of accidents on telecommunication networks caused by legal entities and individuals shall be reimbursed by them in the procedure established by the legislation. According to **Article 1040** of the Civil Code of the Republic of Uzbekistan, protection of exclusive rights to objects of intellectual property may also be exercised by withdrawal of material objects with the help of which exclusive rights are violated, and material objects created as a result of such violation; obligatory publication about the committed violation with the inclusion of information about who owns the infringed right; **Article 65** of the Law of the Republic of Uzbekistan "On copyright and related rights" also specifies the protection of copyright and related rights. Thus, under the Act, the author, owner of related rights or other holder of exclusive rights has the right to demand from the infringer: recognition of rights; restoration of the situation that existed before the violation of the right and termination of actions that violate the right or threaten to violate it; compensation for losses in the amount of the income not received, which the holder of the right would have received under normal conditions of civil turnover if his right had not been violated. If the infringer has received income as a result of the violation of

		copyright or related rights, the right holders shall have the right to claim, along with other losses of lost profit in the amount not less than that of that income; payment of compensation in lieu of damages, paid regardless of the fact of causing the damages, based on the nature of the violation and the degree of guilt of the infringer, taking into account the business customs; It should be noted that **Article 149** of the Criminal Code of the Republic of Uzbekistan provides criminal liability for violation of copyright. Thus, based on this article, attribution of authorship, coercion to co-authorship of intellectual property objects, as well as disclosure without the consent of the author of information about these objects prior to their official registration or publication, shall be punished by a fine from twenty-five to seventy-five minimum wages or deprivation of a certain right for up to five years, or correctional work for up to three years or arrest for up to six months.
6.	What takedown obligations do the platform operators have? (Discussion on the platform operators' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	**Article 18** of the Rules of e-commerce, approved by the Cabinet of Ministers of the Republic of Uzbekistan from June 2, 2016 № 185 stress that an information intermediary is not obliged to control or check the authenticity of transmitted, received, stored electronic documents and electronic messages, as well as their compliance with the legislation, unless otherwise provided by the legislation or the contract. **Article 18** of the Law of the Republic of Uzbekistan on "TELECOMMUNICATIONS" No. 822 – I states that operators and providers operating on the territory of the Republic of Uzbekistan shall provide installation and operation of equipment used for carrying out of operatively-search measures on telecommunication networks at their own expense, as well as provide measures on prevention of disclosure of organizational and tactical methods of carrying out the mentioned measures. Quantity and composition of technical means and equipment used for carrying out of operative-search actions on telecommunication networks shall be coordinated by operators and providers with the bodies engaged in operative-search activity.

		In case of use of networks or means of telecommunication for criminal purposes, which are detrimental to the interests of an individual, society and the state, the functioning of such networks or means of telecommunication shall be suspended. **Article 21** of the aforementioned law highlights that the operators and providers shall have the right to suspend provision of services to users in case of violation of the established rules on use of telecommunications and to reimburse losses incurred through the fault of legal entities and individuals.
7.	Discussion on the takedown procedure i.e the procedures / steps.	Although there is no step-by-step procedure stipulated in the legislation, we recommend to take the following steps: 1) to send a cease letter to the owner of the content, if possible 2) where information on the owner of the infringing content is not available or it is unreasonable to send individual demands, it is advisable to see if the intermediary has its takedown policies and respective forms; 3) where available and reasonable, a takedown notice should be lodged with the intermediary 4) further negotiations and communications with the infringer or the intermediary should be aimed at taking down the infringing content 5) if no results achieved by soft measures of if there is a clear repeated infringement taking place where there is a very low chance to resolve the issue amicably, the case should be taken to the Antimonopoly committee, the court and the “Uzcomnazorat” state inspection/the Ministry for Development of IT and Communications
8.	Are there any forthcoming changes to the law / regulations in relation to intermediary liability / takedown policies / practices?	The project on “AMENDMENTS AND ADDITIONS TO THE LAW OF THE REPUBLIC OF UZBEKISTAN "ON ELECTRONIC COMMERCE" ID-1556 is under consideration. Although it does not address intermediary liabilities and takedown policies clearly, it sets out the obligations of the parties.

9.	General comments on the current legal framework (Are there any interesting case studies or identified problems/issues).	Current legal framework has numerous loopholes, and thus, fails to address the issue properly. Takedown policies on e-commerce are not developed and require many amendments so that they can comply with international standards and meet expectations of all parties.

Vietnam

Contributor: Thomas Treutler (Tilleke & Gibbins); Waewpen Piemwichai / Diep Thi Bich Le / Duc Anh Tran (Tilleke & Gibbins Vietnam Office)
Coordinator: Timothy Siaw (Shearn Delamore & Co.)

No.	Main Points	Answer
1.	Discussion on the general legal framework and scope of the laws governing e-commerce.	Generally, e-commerce transactions are regulated by the provisions of different laws, including but not limited to: - Law on E-transaction No. 51/2005/QH11 dated 29 November 2005; - Law on Commerce No. 36/2005/QH11 dated 14 June 2005; - Law on Protection of Consumer Rights No. 59/2010/QH12 dated 17 November 2010; and - Law on Advertising No. 47/VBHN-VPQH dated 10 December 2018. Depending on the nature of e-commerce activities, there will be separate legal instrument governing, including but not limited to: - Decree No. 52/2013/ND-CP on e-commerce, as amended and supplemented by Decree No. 08/2018/ND-CP dated 15 January 2018; - Decree No. 72/2013/ND-CP on the management, provision and use of Internet services and online information, as amended and supplemented by Decree No. 27/2018/ND-CP on e-transactions in financial activities; - Decree No. 35/2007/ND-CP on e-transactions in banking activities; - Circular No. 47/2014/TT-BCT on management of e-commerce websites, as amended and supplemented by Circular No. 21/2018/TT-BCT dated 20 August 2018; and - Circular No. 59/2015/TT-BCT on the management of e-commerce activities via applications on mobile devices, as amended and supplemented by Circular No. 21/2018/TT-BCT dated 20 August 2018.
2.	What intermediary liabilities do the platform operators hold? (Discussion on the possible liabilities faced by platform operator i.e.	Intermediary liabilities of platform operators: Under various legal instruments, platform operators hold the following intermediary

	contractual liabilities, personal data protection or intellectual property. Please include if there are any defences available for intermediaries.)	liabilities: (i) timely take necessary measures to stop access to, or delete, illegal information at the request of competent state agencies; (ii) cease leasing digital information storage space to parties if they discover, or are informed by competent state agencies, that the stored information is illegal; (iii) ensure information confidentiality for organizations and individuals who lease information storage space; (iv) must obtain the consent of people before collecting, processing and using personal data of other people in the network environment; (v) not provide, post or transmit (including not allow platform users to post/share in the platform) information with content prohibited by Vietnamese law (notably, information that is propaganda against the State of the Socialist Republic of Vietnam; instigates violent disturbances, disrupts security, or disturbs public order; is humiliating or slanderous; or violates economic management order (collectively "**Prohibited Information**"). If a platform operators discovers or receives a notice from an authorized state body that information is illegal, it must cease making the information available through online searches, removing and/or deleting. In addition, an individual has the right to request that anyone who stores his or her personal information check, correct or delete such information. Defences available for intermediaries: Currently, there is an unresolved conflict among various pieces of Vietnamese legislation as to whether intermediary platform operator should have immunity from user's content posted/shared on its platform. On one side, the IT Law, which is the law governing the application and development of information technology in Vietnam, does provide immunity from liability, i.e., a safe harbour regime, for intermediary services providers (including Internet Service Providers, cloud storage service providers, intermediary platform operators, etc.) in certain conditions. According to the IT Law, intermediary service providers are not liable for third-party illegal contents as long as they remove the contents at the request of either a competent authority or an individual, if the content is related to his/her personal information. In addition, intermediary service providers are not responsible for monitoring or supervising other parties' digital information or for investigating breaches of the law arising from the process of transmitting or storing digital information of other

		organizations and individuals, unless an authorized state body so requests. However, the foregoing safe harbor defense will not apply if the intermediary service providers: (i) modify the content of the information posted on their platforms; (ii) fail to comply with regulations governing access or updating content; (iii) illegally collect data via the temporary storage of information; or (iv) disclose confidential information. On the other side, the Law on Cybersecurity, by contrast with the foregoing safe harbour regime under the IT Law, requires all websites, web portals (including intermediary platform) or specialized pages on social networks of agencies/organizations/individuals to: (i) not provide, post or transmit Prohibited Information; (ii) prevent the sharing of Prohibited Information; and (iii) remove the Prohibited Information within 24 hours upon receiving notice from relevant authorities. Accordingly, it could be interpreted that the intermediary platform has the responsibility to proactively take administrative and technical measures to prevent, detect, combat and remove Prohibited Information posted/shared on the platform by its users. Given the foregoing conflict of law, there is an unresolved tension between the safe harbour regime provided by the IT Law and the obligations of websites/web portal (including intermediary platform) under the Law on Cybersecurity to proactively monitor, prevent dissemination and remove Prohibited Information. Thus far, there is no court precedent resolving this conflict. However, in our opinion, as the provisions under the Law on Cybersecurity are specifically applicable to websites and web portals, while the safe harbour regime provided by the IT Law is generally applicable to all types of intermediary service providers, it is likely to us that the provisions under the Law on Cybersecurity may prevail over the safe harbour regime in this context.
3.	Whether brand owners have the right to request/demand for disclosure of the details of the alleged infringers (including, name, contact details, address, bank details) from the platform operators. (Discussion should include the relevant grounds for the request/demand, impact of personal data protection laws, the governing laws and	No, under the prevailing laws, only the state agencies such as Inspector of the Ministry of Information and Communications ("MIC") and Inspector of the Ministry of Culture, Sports and Tourism ("MOCST"), the courts or the polices have the rights to request/demand for disclosure of the details of the alleged infringers (including, name, contact details, address, bank details) from the platform operators).

	regulations and the defences available for the platform operators)	
4.	What are the general applicable laws and the scope in relation to takedown policies? (Related laws/regulations/directions/order and its applicability to takedown policies of IP rights)	The main applicable laws in relation to take down policies include Joint Circular 07/2012/TTLT stipulating duty of enterprises providing intermediary service in protection of copyright and related rights in the internet and telecommunication networks environment ("Joint Circular 07"); Decree 72/2013/ND-CP on management, provision, and use of internet services and online information ("Decree 72"); Circular 38/2016/TT-BTTTT specifying cross-border provision of public information ("Circualr 38"); and Law on Cybersecurity No. 24/2018/QH14 ("Law on Cybersecurity"). Generally, the scope of takedown policies include, upon request from relevant authorities, the intermediary service providers (including platform operators) must remove within the time prescribed by law illegal information posted/shared on their services, including content related to pornography, the incitement of violence, obscenity, depravity, crime, social evils, undermining national security, social order, safety and fine traditions and customs, content harmful to children, defamation (including false information, information that slanders or causes reputational damage, and false information, which violates the lawful rights and interests of other parties), IP infringement of trademarks or copyrights, and spreading viruses and harmful software. Moreover, it important to note that, in case of failure to comply with the authority's takedown notice, in addition to being subject to monetary fine, the platform operator could also be subject to mandatory storage of customers' / platform users' data in Vietnam ("**Data Localization requirement**"), which may limit the platform operator to transfer the customers'/platform users' data to be processed and/or stored outside of Vietnam. Currently, the Ministry of Public Security ("**MPS**") is drafting regulation to implement Data Localization Requirement ("**Draft Decree**"). According to the current version of the Draft Decree, both domestic and foreign providers of online services specified by the Draft Decree (including intermediary platforms, such as e-commerce platform, social networks and other online services with online chat, voice and text functions) would need to comply with the Data

		Localization Requirement if (i) their services were used to commit violations of Vietnam's laws (such as posting/disseminating Prohibited Information) and (ii) they have received a warning from the MPS (such as takedown notice) but have failed to remedy the situation. In such case, the MPS will send an official notification demanding such online service provider to comply with the Data Localization Requirement in Vietnam. The company receiving the data localization notice will have six months from the date it received the notice to comply with the Data Localization Requirement. Moreover, if the company subject to the Data Localization Requirement is a foreign company (i.e., incorporated and operates outside of Vietnam), it would also be required to set up a representative office in Vietnam. However, it is worth noting that as the Draft Decree has not yet been finalized/promulgated; details of the regulations could be changed in its final/promulgated version. According to reports, after revising the Draft Decree several times, the MPS aims to finalize it and promulgate it in 2020.
5.	What takedown obligations do the e-commerce sellers have? (Discussion on e-commerce sellers' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	Under Law on e-commerce, e-commerce sellers have obligations to comply with the laws on payment, advertising, promotion, protection of intellectual property rights, protection of consumer interests and other relevant laws when selling goods or providing services on the e-commerce trading floor. In other words, the sellers must not supply products that are counterfeit goods or goods/services infringing upon intellectual property rights, or goods/services in the list of goods and services banned from business. Upon request from the platform and/or the relevant authorities, the sellers must take down such listings and/or any information prohibited by laws.
6.	What takedown obligations do the platform operators have? (Discussion on the platform operators' obligations / defences in relation to takedown practices from all perspectives i.e. general / intellectual property)	As mentioned above, the platform operators have to the obligations to takedown all illegal contents that appear on their platform at the request of the authorities. In terms of intellectual property, Vietnamese law requires platform operators to protect copyrights and other intellectual property rights. For example, under Article 5 of Joint Circular 07, platform operators must remove and delete content that violates copyright and related rights, when it receives a written request from Inspector of MIC and MOCST, or other state agencies as prescribed by law. It may also be required to supply information on customers using

		intermediary services at the request of Inspector of the MIC, the Inspector of the MOCST, or other competent state agencies.
7.	Discussion on the takedown procedure i.e the procedures / steps.	Vietnamese laws only regulate on the takedown procedure, as requested by competent authorities. In particular, the law requires only that a notice sent from competent authorities, such as MIC or MOCST, be made in writing or by electronic means (Article 5.3 of Joint Circular 07; Article 23d.2(c) of Decree 72; Article 5.1 of Circular 38). However, the law is silent on the notice's form. Upon receipt of notice from competent authorities, an intermediary platform operator is required to locate the information, remove Prohibited Information and/or implement the requested relief within 24 hours (Article 26.2(b) of the Law on Cybersecurity; and Article 5.1 of Circular 38). In general, the competent authorities have the right to order both domestic and foreign intermediary platform operators to remove content (Article 18.3(b) of IT Law; Article 5.3 of Joint Circular 07; Article 23d.2(c) of Decree 72; Article 5.1 of Circular 38).
8.	Are there any forthcoming changes to the law / regulations in relation to intermediary liability / takedown policies / practices?	We are not aware of any forth coming changes to the law/regulations in relation to intermediary liability / takedown policies / practices in Vietnam, except the Draft Decree implementing the Data Localization Requirement (pease refer to our response to Question 4 for more information).
9.	General comments on the current legal framework (Are there any interesting case studies or identified problems/issues).	In general, the current takedown policies under the Vietnam's law has brought many difficulties for the brand owners to prevent infringing contents/information/products from online platforms. As mentioned, the perquisite for the illegal contents to be removed is at the request of state authorities, in practice, is very cumbersome and time-consuming to obtain such request from the authorities, thus, the illegal contents in many cases are not timely removed as expected by the brand owners.

China

Contributor: Riccardo Ragonese (Red Points)

TAKEDOWN POLICIES AND PRACTICE

A precondition to understand take down policies and practices of online operators in China as well as the rights brand owners can appeal to, is to have a clear vision of the legal framework regulating e-commerce.

For this purpose, we will cover the legal sources in general before delving into the specifics of the different platforms, to then assess if their policies are consistent with the legal provisions.

1. The legal framework

1.1 Scope of the law and relevant subjects.

E-commerce in China is regulated by the new e/commerce law, in force from January 1, 2019[3].

Aim of the law is to protect the legitimate rights and interests of all parties of e-commerce, regulate e-commerce behaviour, maintain market order, and promote the sustainable and healthy development of e-commerce.[4]

Its scope regards "electronic commerce", defined as the sale of goods and services via Internet. Conversely, areas such as financial products and services that use information networks to provide services related to news, audio and video programs, publications, and cultural products are excluded from the coverage of the law.[5]

E-commerce operators are defined broadly by art.9 to include natural, legal and unincorporated organizations engaged in the business of selling goods or providing services online. On the basis of the role they play in e-commerce they are divided as follows:

1. **Platform operators. (platforms)** These are entities that pronavide the infrastructures for online vendors, act as intermediaries for transactions, or provide information to parties in transactions that enable them to carry out business activities. Taobao or Jindong are such examples.

2. **Operators on e-commerce platforms.** (sellers) These refer to vendors that sell goods or services on e-commerce platforms.

3. **E-commerce operators.** (sellers) This residual category includes entities that sell goods or services through their own websites or different network services, such as social media. (Wechat, Douyin).[6]

1.2 Obligations of the sellers

Both the **Operators on e-commerce platforms** and the **E-commerce operators** share the **obligation to register as market entities**.

---

[3] The full text of the law can be read at https://duxiaofa.baidu.com/detail?searchType=statute&from=aladdin_28231&originquery=%E7%94%B5%E5%AD%90%E5%95%86%E5%8A%A1%E6%B3%95&count=89&cid=e1a5b5a1b0206935b4fed90e217d94dd_law

[4] Art.1 of the Chinese e-commerce Law

[5] Art.2 of the Chinese e-commerce Law

[6] This broad definition allows for an extension to the applicability of the law beyond the traditional marketplace sellers to newer forms of online sale such as daigou or individuals using Social media to sell goods.

The only exceptions from the obligation are the cathegories contemplated in article 10: individuals selling self-produced agricultural and sideline products, household handicraft products, individuals using their skills to engage in convenient labor services and sporadic small-scale transactions that do not require a license according to law, and do not require registration in accordance with laws and administrative regulations.

The fact that the list of exceptions is closed and the one of the subjects with the obligation is designed in very broad terms is a clear indication of the will of the legislator to include new forms of online sales that may arise in the future in the latter category unless the occasional nature of the transaction directs in the opposite sense.

Another requirement set by the law is that all e-commerce operators must **report and pay taxes according to applicable laws and regulations**. [7]

Not paying taxes constituted in the past a competitive advantage for online sellers respect to physical shops, and the new regime, together with rising delivery costs, can erode the margin of earnings and therefore the volume of sales of platforms such as Taobao.[8]

To improve transparency and traceability e-commerce operators are subjected to a series of rules, such as publishing their business license information, or alternatively the reasons for exemption on a prominent position on their homepages Logo and, if the information specified in the preceding paragraph changes, to update the publicized information in a timely manner.[9]

In case of termination the seller shall continue to publish relevant information on a prominent position on the front page 30 days in advance.[10]

E-commerce operators shall disclose the information of commodities or services in a comprehensive, true, accurate and timely manner to protect consumers 'right to know and choose. Abstaining from engaging into false or misleading commercial propaganda in the form of fictitious transactions or fabricated user evaluations to deceive or mislead consumers.[11]

Simply put merchants are required to disclose any clauses or bundles they have placed on their offers and cannot presume the buyer's consent.

The new legislation will also prevent fake reviews, including not only those written by hired agents, but also the ones written by customers in exchange for monetary rewards.

Operators shall clearly state the method and procedures for the refund of the deposit, and shall not set unreasonable conditions for the refund of the deposit.

1.3 General obligations of the platform operators

The set of obligations and responsibilities for e-commerce platform operators is also extended by the new law. Platforms should require operators who apply to enter them to sell commodities or provide services to submit real information such as their identities, addresses, contact information, and administrative licenses for verification and registration, establish registration files, and periodically check and update.[12]

---

[7] Art. 11

[8] In this sense: Jung C., 24.9.2018, "How Would the New Chinese E-commerce Law Change Taobao?"

https://pandaily.com/how-would-the-new-chinese-e-commerce-law-change-taobao/

[9] Art. 15

[10] Art. 16

[11] Art. 17

[12] Art.27

These pieces of information must be shared by the platform operator in the cases contemplated by the law.[13]

According to the law platforms operators **should take all the necessary measures to prevent network illegal and criminal activities**,[14] provide quality assurance of goods and services, protection of consumer rights and interests, and protection of personal information[15].

If the operator of the e-commerce platform knows or should know that the goods or services provided by the operator on the platform do not meet the requirements for ensuring the safety of the person and property, or other acts that infringe on the legitimate rights and interests of consumers, and fail to take the necessary measures, **the platform shall bear joint and several liabilities**. [16]

1.4 Obligations of the platform operators concerning Intellectual Property

Additionally, in articles 42-46 the new law draws the responsibility of the platforms with regards to Intellectual Property protection.

In details it makes mandatory for E-commerce platform operators to **establish rules for intellectual property protection**[17] **and to cooperate with IP owners to protect intellectual property rights**.

Under the new regime Intellectual property rights holders who believe that their intellectual property rights have been infringed have the right to notify operators of e-commerce platforms to take necessary measures such as deleting, blocking, disconnecting links, terminating transactions and services. [18]

The notice shall include preliminary evidence of infringement.

After receiving the notice, the operator of the e-commerce platform shall take necessary measures in a timely manner and forward the notice to the seller.

If the necessary measures are not taken in time, the platforms themselves shall be jointly and severally liable with the seller.[19]

After receiving the take down request the sellers may submit a declaration of no infringement (counternotification) to the operators of the e-commerce platform. The statement should include preliminary evidence of no infringement.

After receiving the statement, the operator of the e-commerce platform should forward the counter notice to the intellectual property right holder who issued the notice, and inform him that he can file a complaint with the relevant competent authority or file a lawsuit with the people's court. If the operator of the e-commerce platform does not receive the notice that the right holder has filed a complaint or prosecution within 15 days after the transfer statement reaches the intellectual property right holder, it shall terminate the measures taken against the seller.[20]

The law also opens the door to a joint liability of platforms on the ground of missed activation when the operator of the e-commerce platform knows or should be aware of the infringement of intellectual property

[13] Art.28
[14] Art. 30
[15] Art. 32
[16] Art.38
[17] Art 41
[18] Art.43

[19] The protection works also in the opposite direction: if a wrong notice is issued in bad faith, causing losses to the operators on the platform, it shall double the liability for compensation. (art.43)

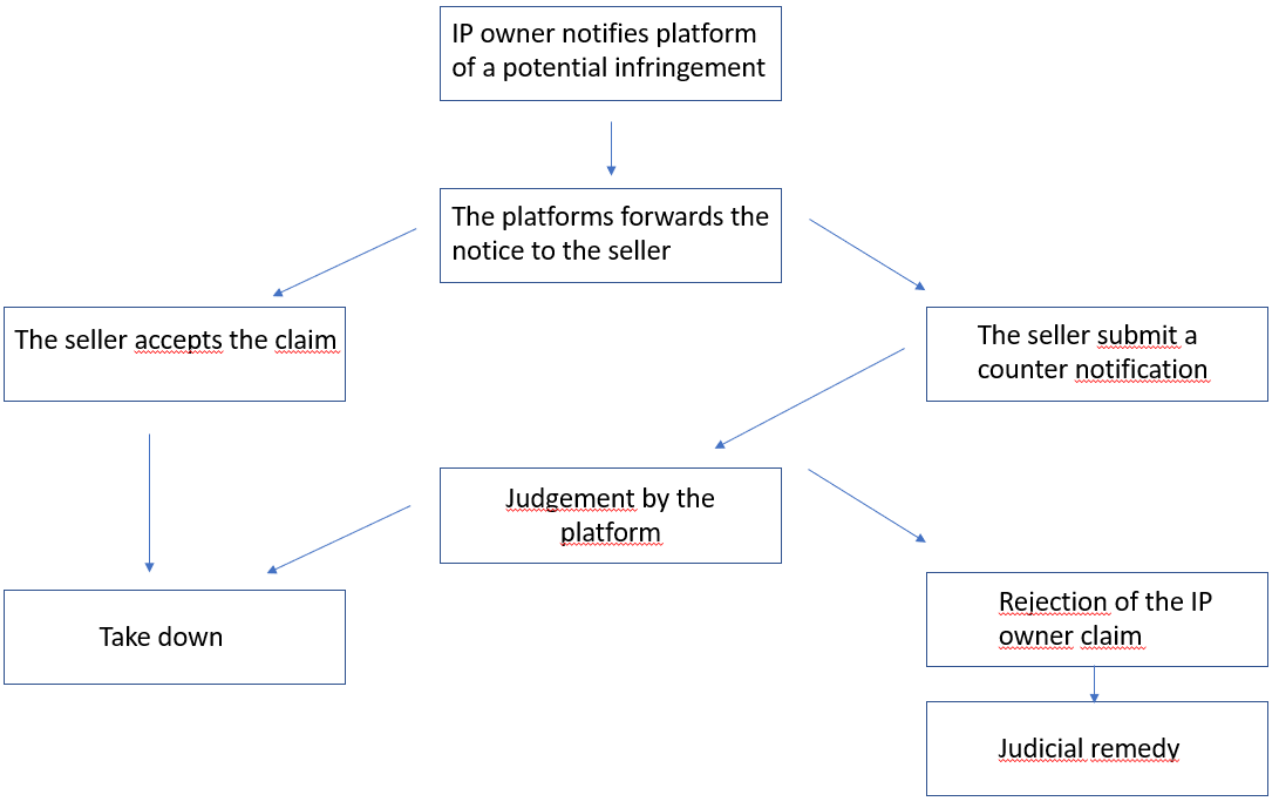
[20] Art. 43

rights by the operators on the platform and has not taken necessary measures such as deletion, shielding, disconnection, termination of transactions and services.

In this case there is no need of the request of the brand owner to start the procedure.

To comply with this requirement some Chinese platforms have established forms of proactive monitoring[21]

Fig.1 IP takedown procedure



1.4 Assessment of the law

The scope for take-downs is broadened by the extension of the liability of the platforms put in place by the new e-commerce law.

For this purpose E-commerce platforms must set up clear rules to protect IP rights, and act on a timely fashion when a violation is notified.

In other words **platforms are not allowed anymore to appeal to the traditional principle of neutrality, and to represent themselves as mere intermediaries in sales but have to answer for the violation perpetrated through them**.[22]

In more details platform operators are now **called to ensure that all the items offered on the platform are not in breach of intellectual property** laws and regulations.

[21] Art. 45

[22] A traditional argument used by platforms before the new e-commerce law was that they were simply providing the infrastructure on which the transaction took place and were therefore not responsible for the misuse of such infrastructures by sellers. Brand owners had to deal with the sellers themselves.

It also compels them to **engage in the disputes between customers and sellers** arising on the platform, with the involved legal risks.

This direct involvement also implies that **E-commerce platforms will now be jointly responsible for the sale of counterfeits through their site**, while previously, only individual sellers were held accountable.

Under the new law, platform operators must answer in a timely manner to reports of violations or risk penalties of up to US$30 million.

By increasing the accountability of the platforms the new law makes it easier for consumers to sue both sellers and the platform for any violation.

Also the responsibilities of sellers are deepened.

In the sense of traceability goes the requirement of a **business registration for retailers** on e-commerce sites.

To sell on the platforms users must first obtain a business license by registering with the State Administration for Industry and Commerce.

If the steps above point to a greater consideration of IP in online transactions some shadow zones still remain.

For example the **lack of specification regarding the standard of evidence** required for the take down or for the counternotifications are configured in very generic terms, leaving them to the discretional evaluation of platform operators.

The same concern exists for **take down time** and **procedure**.

There is no clear deadline for a platform to proceed to take down, as the low simply requires a timely activation, allowing platforms to delay enforcement within certain limits.

There is also no standardised take down procedure and each platforms can set up its own rules, which are not always and the systems put in place across platforms are not always straightforward or efficient.

2. Takedown policies and practices

While the law broadly defines the general framework of the e-commerce regulation, it leaves to the discretionality of the platforms how best to implement the legal provisions.

Unsurprisingly this has lead to a diverse fulfilment across different operators.

We will look into detail to the systems adopted by the biggest e-commerce players, Alibaba and Tencent and evaluate their level of conformity to the provisions of the law.

2.1 The Alibaba group

The Alibaba group doesn't sell goods of its own but provides to third-party merchants a powerful and ramified infrastructure to distribute their products both domestically and internationally.[23]

Therefore the revenue for the platform derives from commission fees and selling ad services.

For small and medium companies leveraging on a centralized, pre-existing structure means huge savings in term of transaction costs, and great advantages on the ground of visibility, which is the root of the popularity of the group.

[23] Paying attention to this aspect is important for establishing which certificate to use. Only platforms selling abroad accept WIPO certificates

The centrality of infrastructure also explains the constant focus for Alibaba in enhancing the integration of its services through a combination of the group own innovations and internalization of features from its western competitors, such as Amazon and Ebay.

In particular integrated payments [24]an internal ads system[25] and quick deliveries[26] are three strong points of Alibaba, which is now striving to expand beyond the market that it traditionally covered.

A traditional weak point of the group was the fact it targeted mainly 1st and 2nd tier cities, allowing rivals such as Pinduoduo to expand in lower tier towns

But Ecommerce is only one of the many facets of the group, whose business also include e-payments (Alipay), video streaming and cloud computing, adding to its solidity.

As of today the Alibaba group is constituted by 7 platforms, each specialized on specific markets and target users.

Since for brand owners understanding these subtleties is key in building an effective IP protection strategy in this section we will provide a guide to understand their individual characteristics.

A first distinction to make is between domestic and international platforms: only the latter accept WIPO certificates, while domestic ones require locally registered trademarks as a condition for take-downs.[27]

In the following we will give a more detailed overview of the platforms that are part of the Alibaba group.

2.2 Domestic Platforms

2.2.1 Taobao

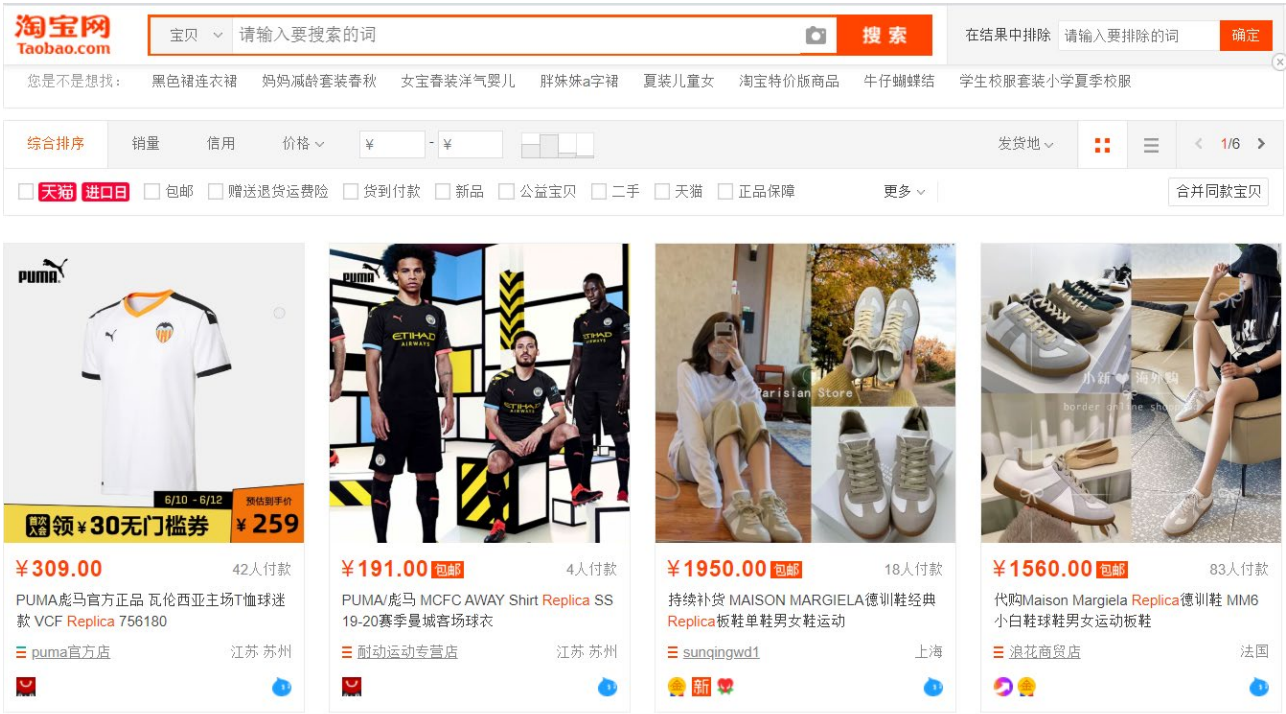
Replicas on Taobao

[24] Alipay is Alibaba integrated payment provider

[25] Alimama

26 To support the expansion of e-commerce Alibaba has invested considerably into logistics. Taobao users expect to receiving goods within a few hours when buying from a merchant in the same city. Cainiao is the logistics infrastructure behind the Group and its role is to ensure that all domestic deliveries are completed within 24 hours and aiming at 72 hours for international deliveries.

[27] The language used by the platform is also a clear indicator if it is meant to foreign or local consumers.



Taobao is a domestic C2C marketplace and the world's largest ecommerce platform.

Constantly ranking as the third domain in China for number of visits it enables its user to have a very extensive visibility and reach for their products.

The possibility of customization of the seller page, allowing for extensive descriptions of the products specific, business driving ads and its being available also in a mobile friendly versions are yet other reasons for the popularity of the marketplace among sellers and users alike.

Many previously unknown brands owe their success and popularity to Taobao.

Unfortunately also counterfeiters spotted the endless potentiality of the platform and flooded it with counterfeits, making it a corner stone for any holistic brand protection strategy.

The fact that Taobao is meant for the domestic market only implies that sellers as well must be based in China and brand owners wanting to take down listings can only rely on Chinese certificates.

In other words an item will be removed only if it infringes a Chinese registered trademark or design right.

Trying to take down listings using international certificates is at the root of the frustration of many brand owners

*2.2.2 **Tmall***

Tmall is a B2C platforms which is second only to Taobao in China, and allows brands to connect with the end-buyers directly, without the involvement of a third party seller.

This allow a greater guarantee of authenticity for buyers and a wider margin of earnings for the brand owner. Tmall to Taobao is in the same relationship that is Amazon to Ebay.

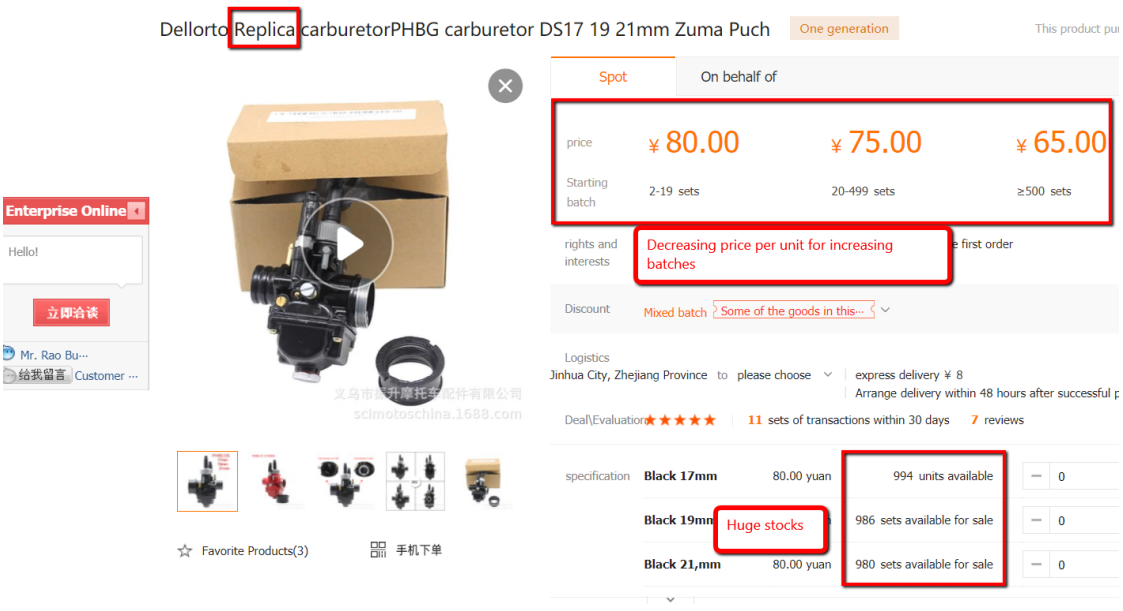
While Tmall listings can be accessed through Taobao, the reverse is not possible in line with the strategy to represent Tmall as a more protected, exclusive environment for shopping.

The platform is domestic[28], meaning that a company selling on it should be registered in China and Chinese should be also the certificates used for enforcement.

Many brands in China sell directly on Tmall and to incentive this trend the platform created a special section, called **Luxury Pavilion**, dedicated to a selection of high end brands.

Consistently with its targeting major brands the level of IP protection on Tmall obeys to higher standards with harsher sanctions for counterfeiters and less bargain offers

2.2.3 1688



This domestic B2B platform is designed for merchants selling in bulk. By means of it manufacturers and suppliers target wholesalers rather than end users.

Many Taobao sellers purchase their stock from 1688 and resell the items to final consumers for an augmented price.

Enforcement on the platform is made difficult by the fact that many items are in a raw state, and customization happens only after the sale.

This means for examples that logos can be engraved on items on the instructions of the wholesale buyers and only then become counterfeits but on 1688 itself there is no infringement to be found.

In this way brand owners will remove the manifestation of the counterfeiting industry but the fucine of them would stay untouched.

It is therefore of the utmost importance for brands seeking protection in China to address 1688 as a priority as it is the origin of many violations.

[28] A small opening in this sense is constituted by **Tmall Global,** which enables foreign shops to sell in China, although its user base is considerably small.

2.2.4 Xianyu

Originally an independent platform within the group, Xianyu has now been integrated within Taobao, and so the enforcement, which is conducted through the Taobao portal.

The C2C Xianyu is specialized in the sale of second hand goods. Take-downs are complicated by the fact that low price cannot be used as a reason for removals because on the basis of the exhaustion of IP rights after the sale of an item the buyer is free to resell it for a lower price. Also the conditions of the items can be bad, complicating a judgement over the authenticity of the product. Overall the burden of proof for brand owners on Xianyu is considerably higher than on Taobao.

Sometimes high volume of stock can be indicators of the fact that an item is counterfeit because is unlikely that a seller possess such a quantity of second hand goods, otherwise a test purchase can be resolutive.

2.3 International Platforms

2.3.1 Alibaba.com

Conceived as an international B2B platform, Alibaba constitutes the international version of 1688 with the purpose of connecting Chinese sellers to the international markets.

It was the first platform to be implemented, testifying of the expansionist aims of the group.

Due to its international nature WIPO certificates are accepted on the platform.

It was thought to open up the platform to US sellers but the trade war between China and the US seems to have slowed down this process.

2.3.2 AliExpress

This B2B platform is the international equivalent of 1688.

Many distributors are active on both platforms when they hold an export licence allowing them to sell abroad.

AliExpress recently opened to non-Chinese sellers from Russia, Turkey, Spain and Italy and the list is likely to expand over time.

The B2B nature is not an hard requirement and retail sales are also supported: a growing number of manufacturers allows very low minimum quantity orders or even single purchases making the platform a destination for dropshippers and small retail businesses together with enterprises.

As normal with international platforms international certificates are accepted on Aliexpress.

2.3.3 Lazada

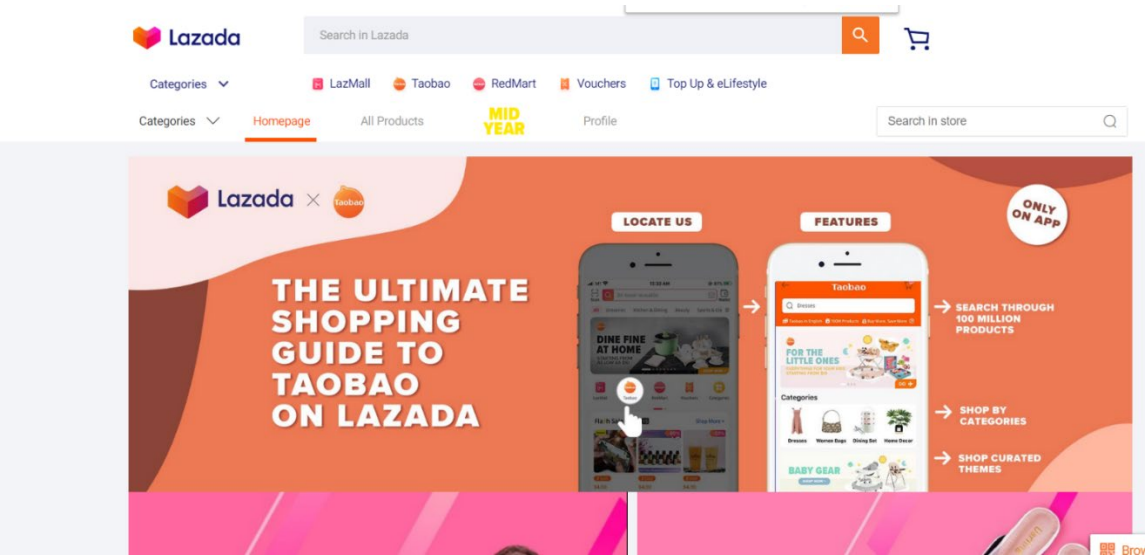
Lazada is, together with Tokopedia, one of the leading ecommerce platforms in South-East Asia, operating in Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam.

It became part of Alibaba in 2016, when the group acquired its controlling stake. Proof of the integration is the fact that as of today all the violations on any Lazada regional website are reported through Alibaba IPP Platform, streamlining the process respect to the past.[29]

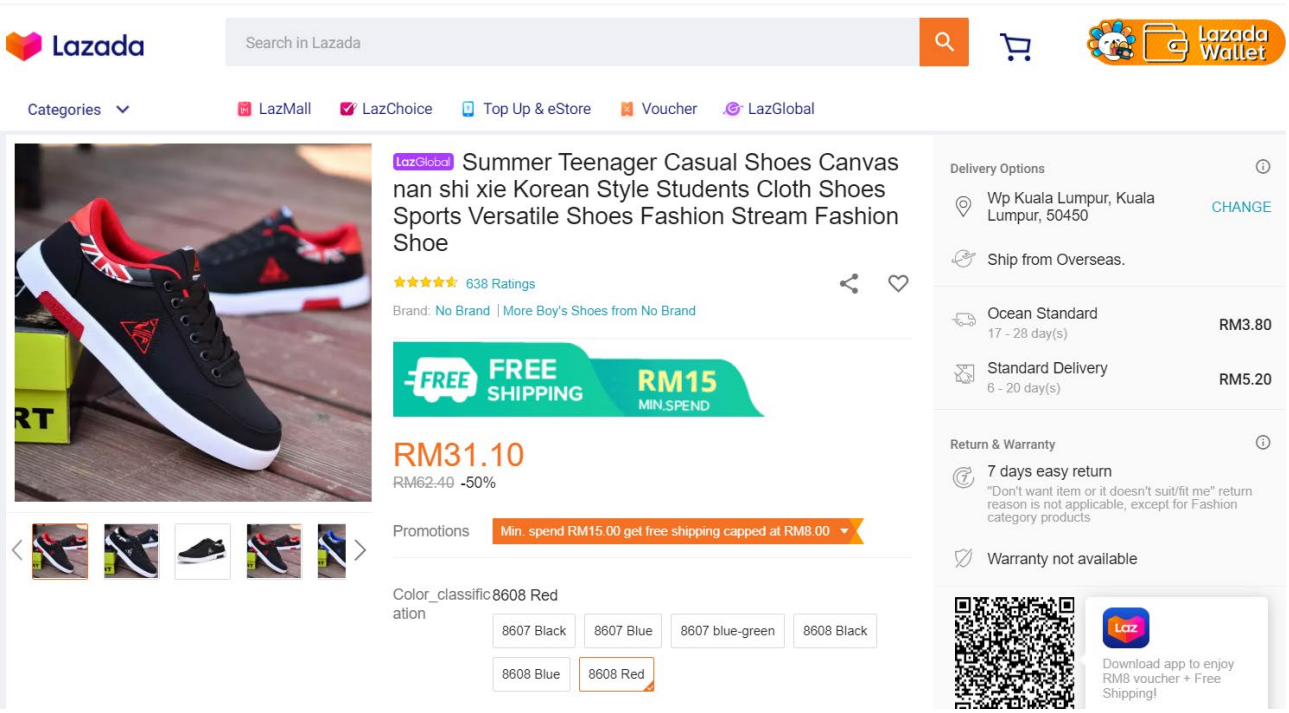
Unfortunately the acquisition made also simpler for Chinese counterfeiters to sell their product in Lazada and we see an increasing number of “Taobao collections” in the South-eastern platform.

Below a proof of the contamination between Taobao and Lazada

[29] Notice of the Launch of Online Portal for Lazada2019-06-25, available at https://ipp.alibabagroup.com/infoContent.htm?skyWindowUrl=notice/20190625/en



Even the layout of the listings is very similar giving Lazada customers an experience very similar to that of Taobao users.



2.4 The Alibaba Group's Brand Protection Tools

Takedown requests for any of the platforms described above can be filed through webform[30], through the Alibaba Intellectual Property Protection portal: "ipp.alibabagroup.com" or the AACA program.

2.4.1 Intellectual Property Protection Platform (IPP Platform)

Between emails and the IPP portal the latter is by far more efficient because provides a single resource for all the different marketplaces and is represented by Alibaba as the proof of its commitment to the protection of IP at every event involving brand owners, trade association and relevant local bodies.

Through the portal brand owners or their representatives can submit, track and escalate IPR infringement issues. The portal also contains training materials ant the group policies.

Understanding them is important not only to successfully take down listings but also to remain part of the 'Good-faith Takedown Program' .

Members of the program enjoy a lowered burden of proof, a reduction of the takedown time and have also access to extra data thought for brand owners.

To obtain membership a brand owner needs to score a success rate of at least 90% when filing over 100 submissions for three-month in a row but can also lose the status if this percentage deteriorates over time.

Obtaining and maintaining the membership is not an easy task due to the variety of reason codes to select from when reporting a violation: Alibaba possess around three times as many reporting reason codes as Amazon.

When a brand owner reports an infringing item selecting an incorrect sub-reason code the filing is counted as an unsuccessful submission, even if the main-reason category was correct.

Even in case a new submission is made for the same item with the correct reason code, the original submission remains on the record as unsuccessful, regardless of the item being taken down by Alibaba for IPR infringement.

[30] https://ipp.alibabagroup.com/complaint/onlineForm/online.htm

2.4.2 Alibaba Anti-Counterfeiting Alliance

Apart from seeking individual membership in the Good Faith Program brands can also go after a collective subscription through the AACA – an association of brand owners using the portal to report violations across the group.

Many types of brands are represented within the group, from fast-moving consumer goods, luxury, fashion and automotive and it is a good strategy for smaller brands to access the good-faith program in this form.

2.5 Take downs on Alibaba platforms

As anticipated there are two ways to take down on platforms belonging to the Alibaba group: through webform or through the IPP portal.

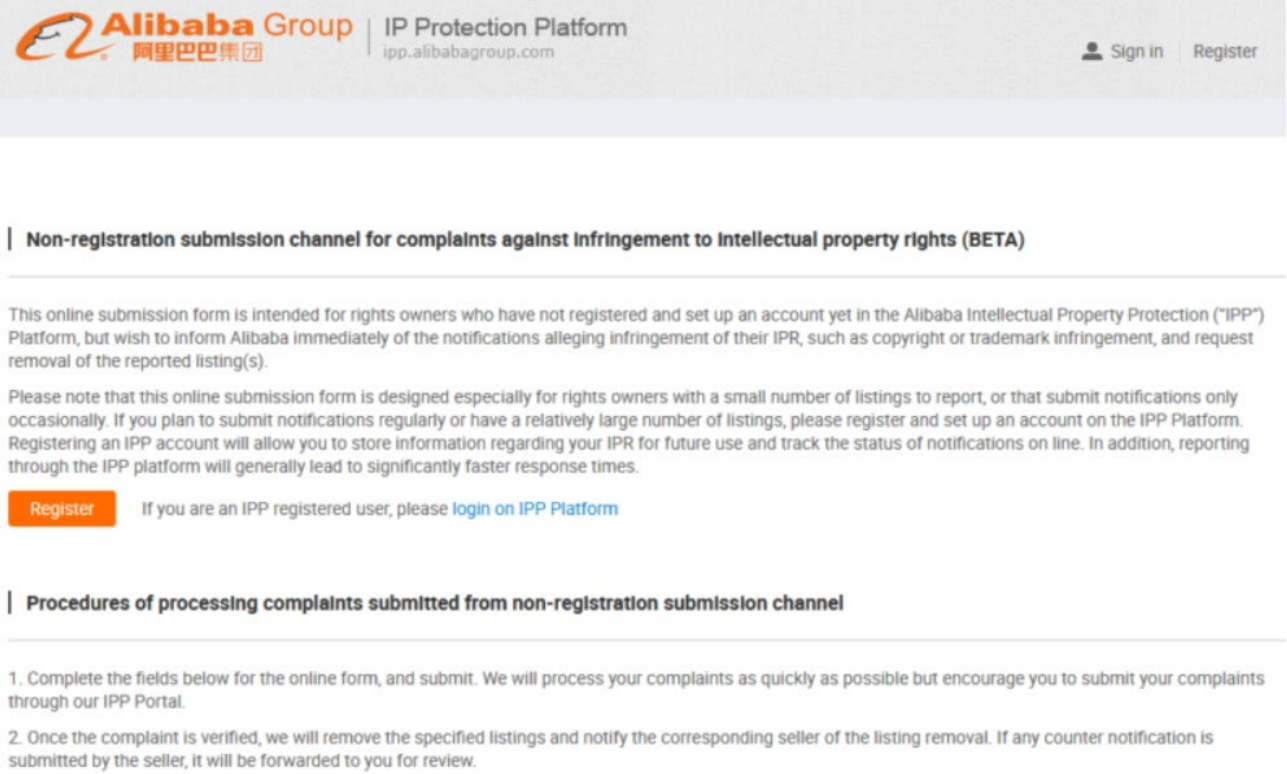
2.5.1 Taking down using the web form

Reporting listings is this way is less efficient than using the portal but has the advantage that no registration is required and can be useful in case of occasional takedowns or in the time before a registration with the portal is completed.

Limitations for rightsholders are a slower takedown time and a limit of 10 infringing URLs per submission.[31]

Note that brand owners registered in the portal cannot use the webform

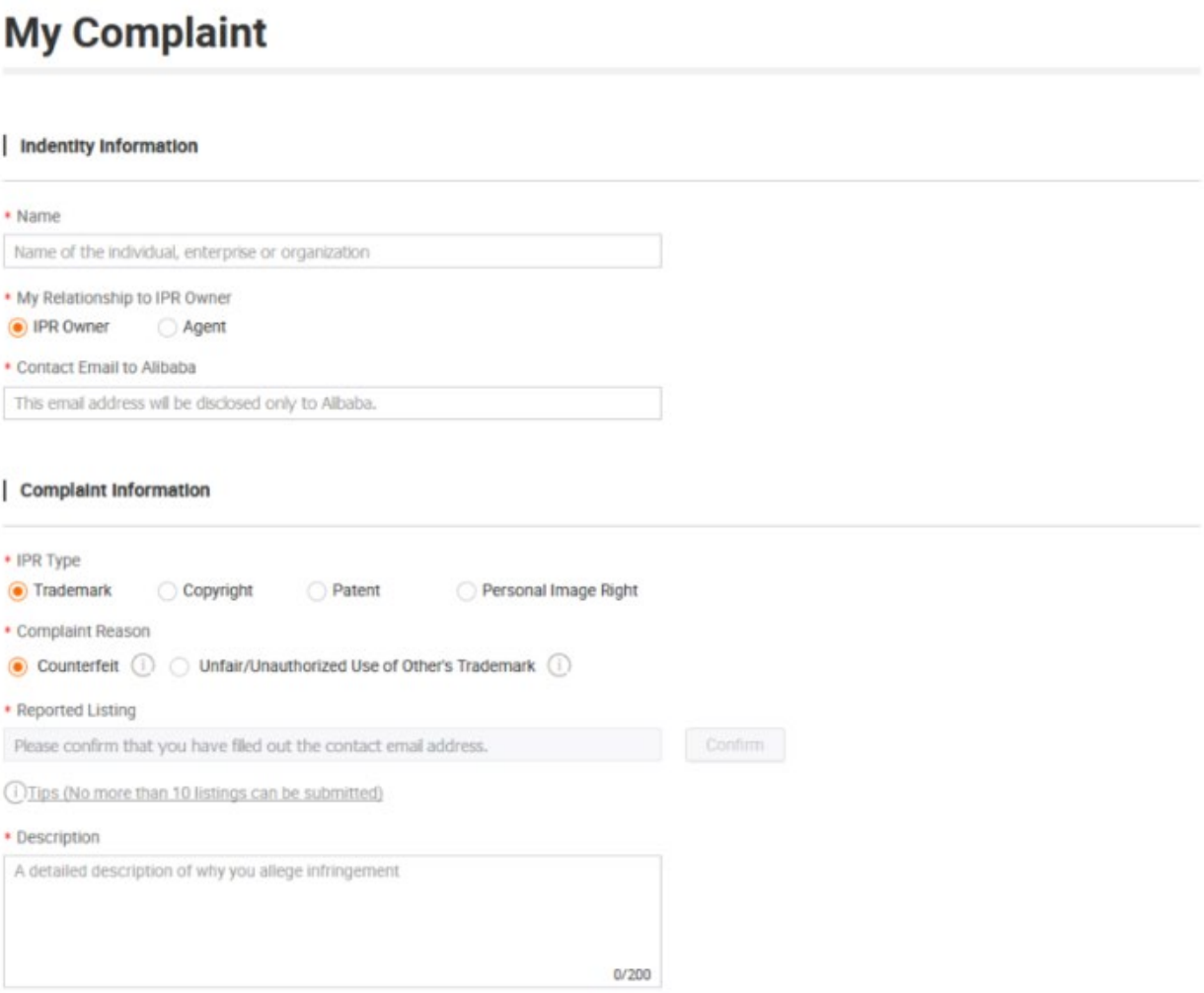
Below we can see how the entry page of the web forms look like and how Aibaba pushes for using the portal instead.



1) Name (it should be the reporter name, even when it doesn't coincide with the IPR owner

[31] Users of the IPP Platform can submit at a time up to 300 listings

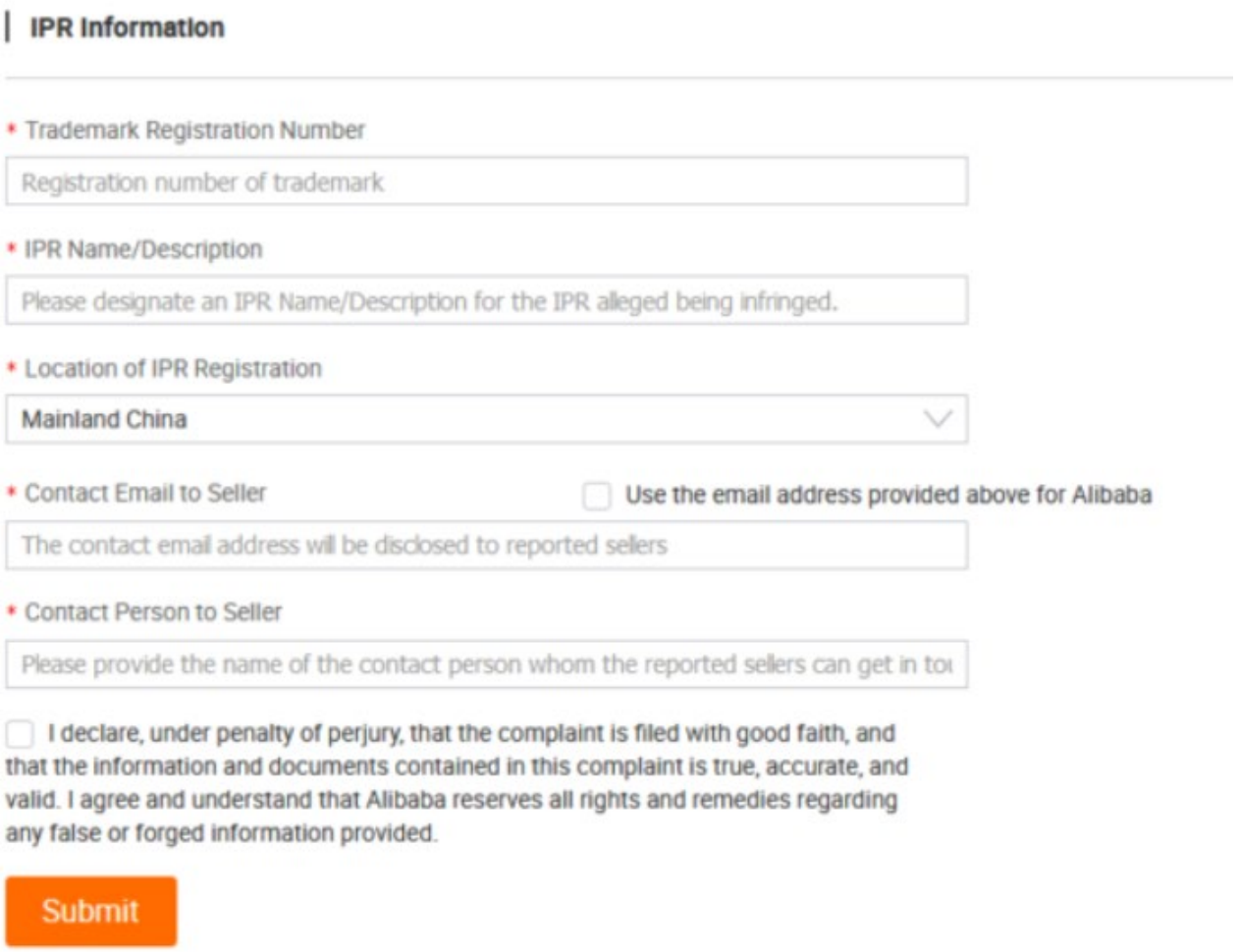
2) Relationship of the reporter with the brand (Can be either IPR owner or agent)
3) Contact email (it will be shared with Alibaba only, not with the infringer.There is however the possibility to add another email address to be shared with the infringer or use the same for both)
4) nature of the complainant (right holder or agent)
5) type of violation (trademark, copyright, patent, personal image)
6) complaint reason (clicking on the “i” icon information is displayed on the meaning of each complaint reason.It is worth to read it as a wrong submission will lead to the rejection of the claim.
7) reported listing
8) description of the infringement



Depending on the IPR type chosen the system will adapt the webform accordingly. For instance if the user select “trademark” as infringement type, the fields ‘trademark registration number’, ‘IPR name’ and ‘location of IPR registration’ will appear.

It is also at this point that the user can select a second email address for contact with the infringer.

Finally, as a condition to proceed the user needs to agree to the terms of the submission, and then click the ‘submit’ button.



At this point the notice is sent to the platform, which will review the claim.

2.5.2 Taking down using the IPP platform

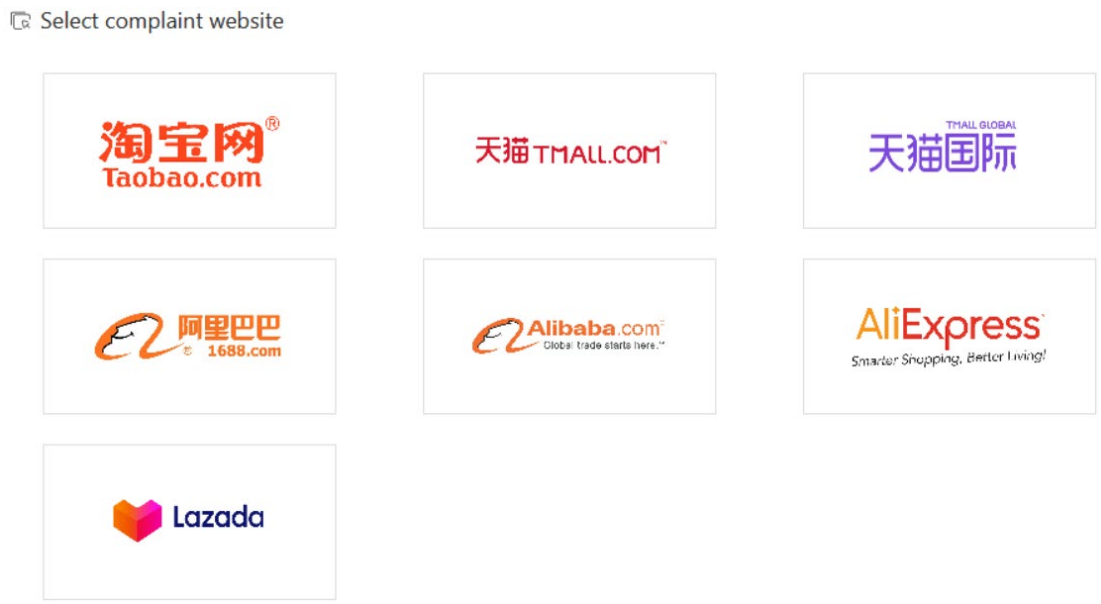
STEP 1: Registration

Using the IPP platform constitutes a fast track for enforcement, with removal requests being processed within 3 working days and high priority infringements taken down in 24 hours or less.

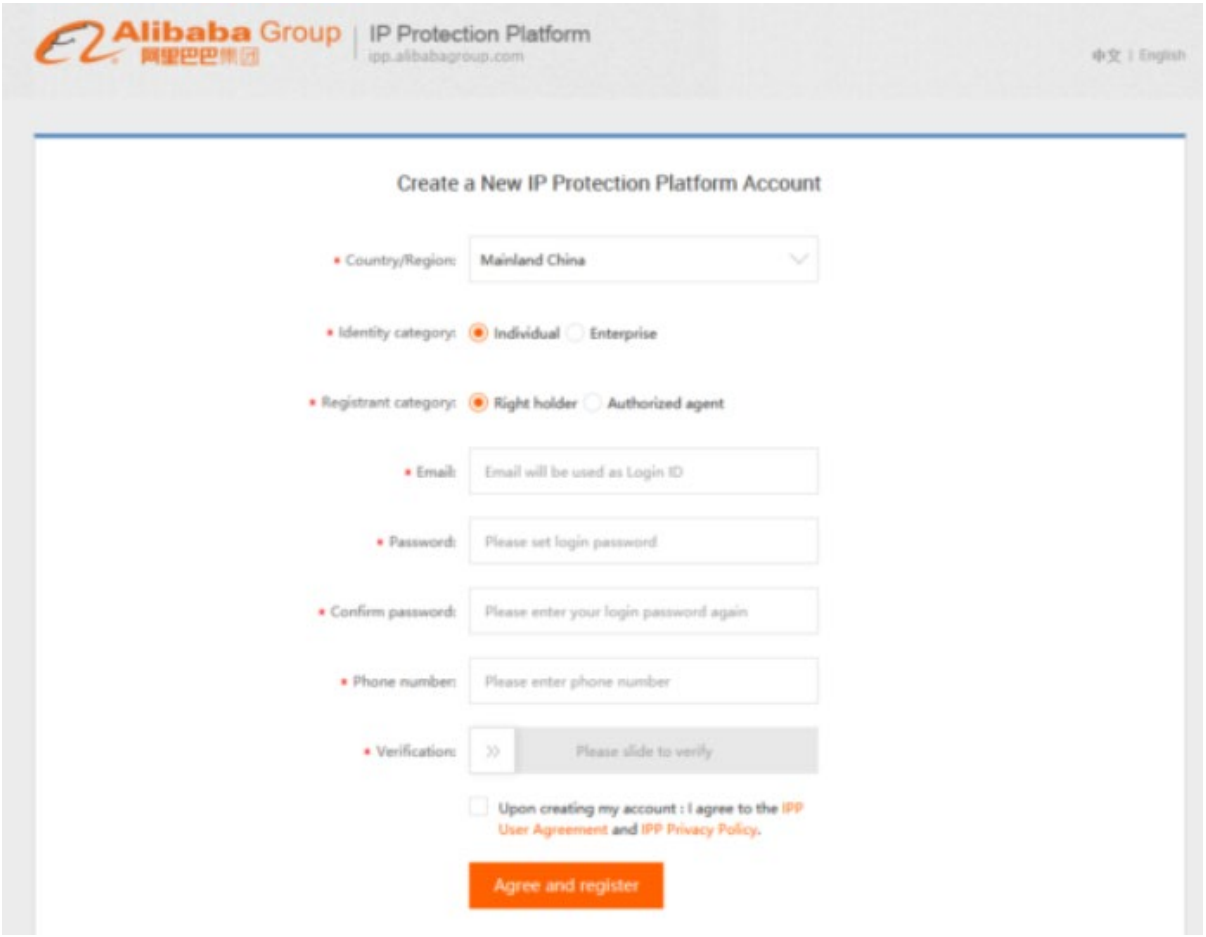
It requires registration that brands can pursue individually or grouped together through the AACA alliance. Instructions are provided at the main page here: https://ipp.alibabagroup.com/

The portal is a comprehensive gateway which allows to report IPR infringements in any of the platforms belonging to the group and follow the outcome of a complaint, in other words the "go-to" space for claims against the e-commerce giant.

As of today the portal covers 7 platforms: Taobao (including Xianyu), Tmall, Tmall Global, 1688, Alibaba.com, AliExpress and Lazada.



To use the platform the user need to register using the form below and indicate:



1) The country where he is based.
2) If he is an individual or a company

3) If he is a ‘Right holder’ or an ‘Authorized agent’.

   If the agent is a rights protection organisation working on behalf of the rightsholder, ‘Individual’ must be selected under identity and agent under registrant.

4) email address (It is recommended to create one dedicated to receiving communications from Alibaba as the sheer number of communications, automated and not, is considerable.

5) Password

6) Agreement to the ‘IPP User Agreement’ and ‘IPP Privacy Policy’

7) click ‘Agree and Register’

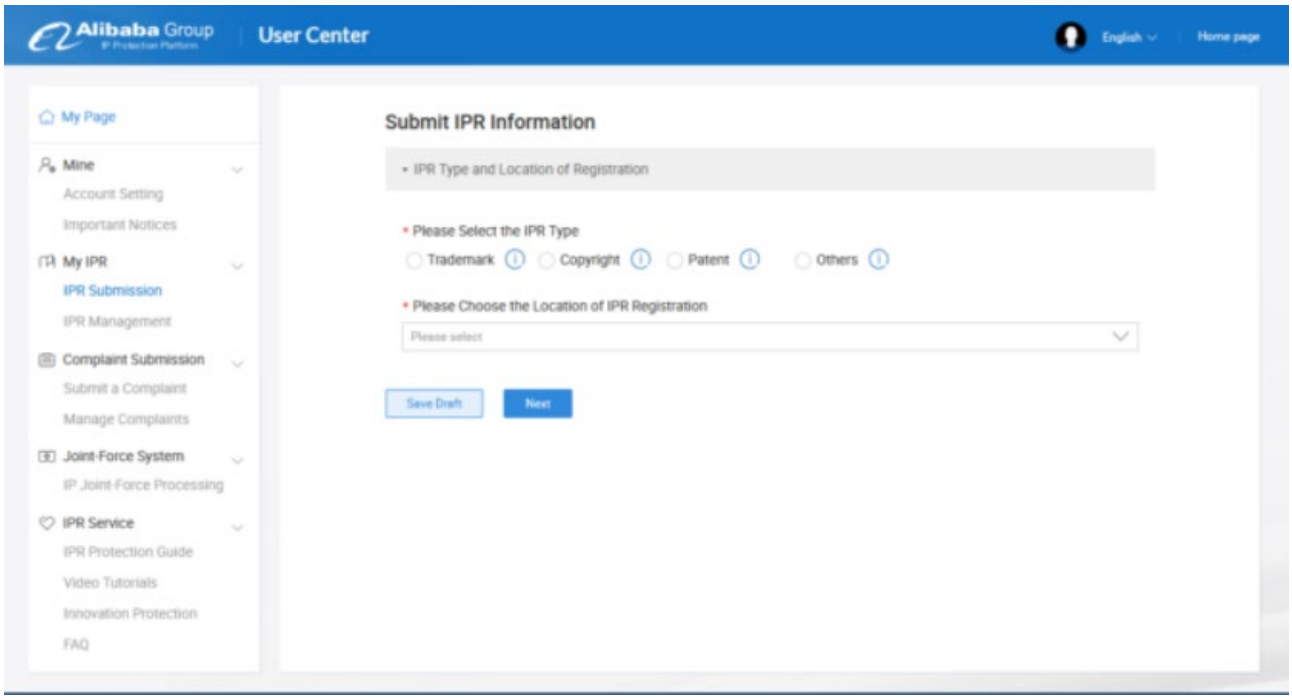
Upon completion of these steps Alibaba will send a verification code to the specified email which the user will need to use to complete registration.

If everything has been done properly the user can now log in into the portal.

Experience suggests that it is convenient for a brand owner to set up a different account on the various platforms of the Alibaba group for monitoring purposes. This will also be useful for test purchases or other intelligence operations.

This account can then be joined to the IPP one for the submission of complaints.[32]

STEP 2: Upload of the IPR



Once the registration is complete the user can upload his Intellectual Property Rights.

[32] The registration is similar to the one with the IPP platform with the user being required to enter an email and password. Afterwards the user needs to complete the identity check up: proof of identity for individuals and proof of company registration for enterprises. Once this is done the IPP portal will be connected to the account for takedown purposes

This can be done through the IPR Submission section within the IPP home page

The choice will be between 'Trademark', 'Copyright', 'Patent' and 'Other'.

Trademarks. For enforcement purposes is worth remembering that only Chinese certificates are accepted on domestic platforms. International platforms accept also WIPO certificates.

Copyrights –The rightsholder needs a statement of ownership to identify the copyright protected works. With this requirement Alibaba sets a middle ground between the Chinese legislation, requiring a registration of copyrights, and the rest of the world, which does not require anything.

Patents – The patent certification must be accompanied by an evaluation report. Designs are also submitted through the patent section

Other – this residual category is meant for rightsholders enforcing through court judgements and any other cases that do not fit in the previously discussed categories.

At this point the user can proceed with the upload [33], click 'next' and fill different forms depending on the rights that he wants protected.

For trademarks, the fields to be filled are 'Name of the trademark', 'Registration number', 'Registrant', 'Expiration date', 'Class' and 'Brand related to the trademark'.

By clicking 'Next' again the section 'Additional information' opens. Here the user can provide information on wether whether the trademark 'has been renewed', 'assigned' or 'altered'.

Then an authorization should be given to enforce the IPR through the account.

The last step is to click 'Submit for verification' and wait for the answer from Alibaba regarding the acceptance of the certificate.

The section 'IPR Management' gives visibility over all all the IPR that have been successfully uploaded.

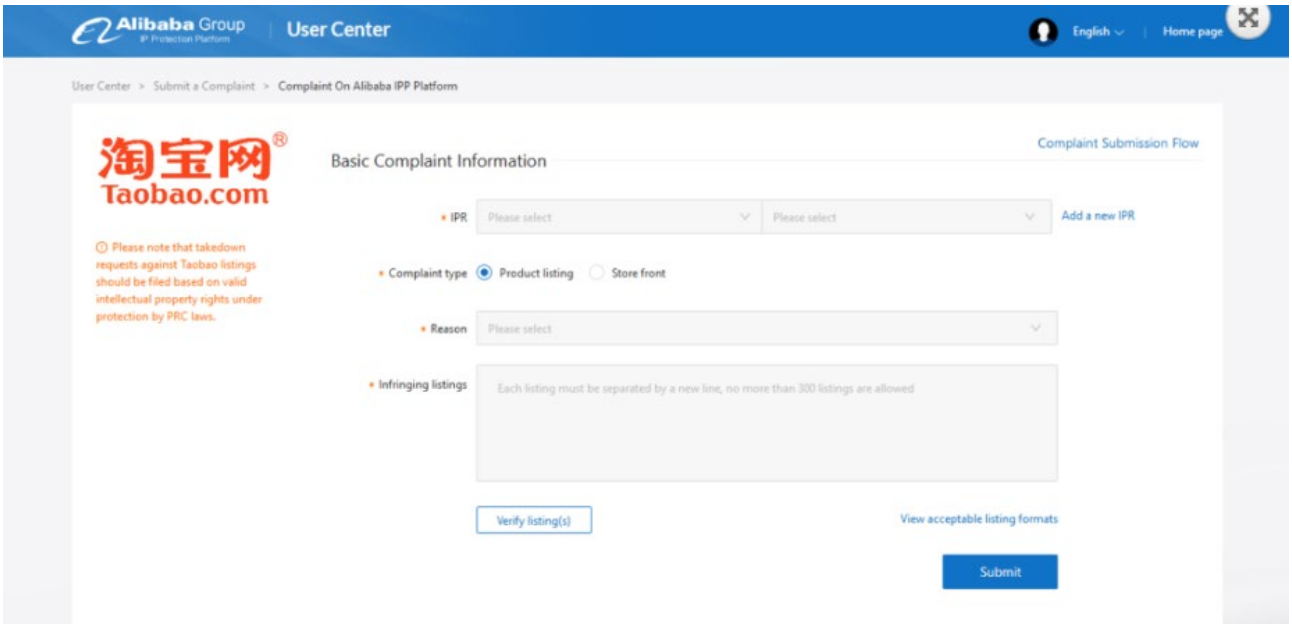
Failed submissions can be viewed as well along with comments from Alibaba, edited accordingly and resubmitted.

STEP 3: Enforcement

Once IPRs have been successfully uploaded, the user can solicit takedowns from the platform.

This is done through the 'Complaint Submission' section in the IPP portal. (Below)

[33] Using the format, file size and file type required by Alibaba.



Here the user need to choose among the different platforms of the group.[34].

For Taobao and Tmall (including Global) the user can report an entire shop rather than an infringing listing, if there is a high volume of infringements in it.

Since in this case the chances of rejection by the platforms are higher is a safer option to report listings from the same shop several times and rely on the three strikes policy of Taobao and Tmall against repeating infringers, which will have the same end results of removing the whole shop.

After the user has decided between reporting product listings or the shop as a whole he needs to select the correct reason code among the many options contemplated by Alibaba. A mistake will not only prevent the successful take-down but also affect the user's rate in the good faith program.[35]

Not only the group is very strict in regard to reason codes but often counterfeiters are aware as well and seek formal gaps to prevent enforcement.

In the box below the user needs to enter the infringing listings each on separate lines and for a maximum of 300 listings every time.

Enforcement practice shows that reporting in smaller batches is more effective reducing the risks that all the 300 listings are rejected together, affecting massively the good faith rate of the user, which requires a success rate of over 90%.

The button"verify listings" allows to check that the listings are still online and have the correct URL structure.

Once all the fields above have been completed the user needs to fill the 'Supplement infringement reason(s)' box giving information about the ifringements. It is important to note that if the infringers are reported in bulk they should all be the same type.

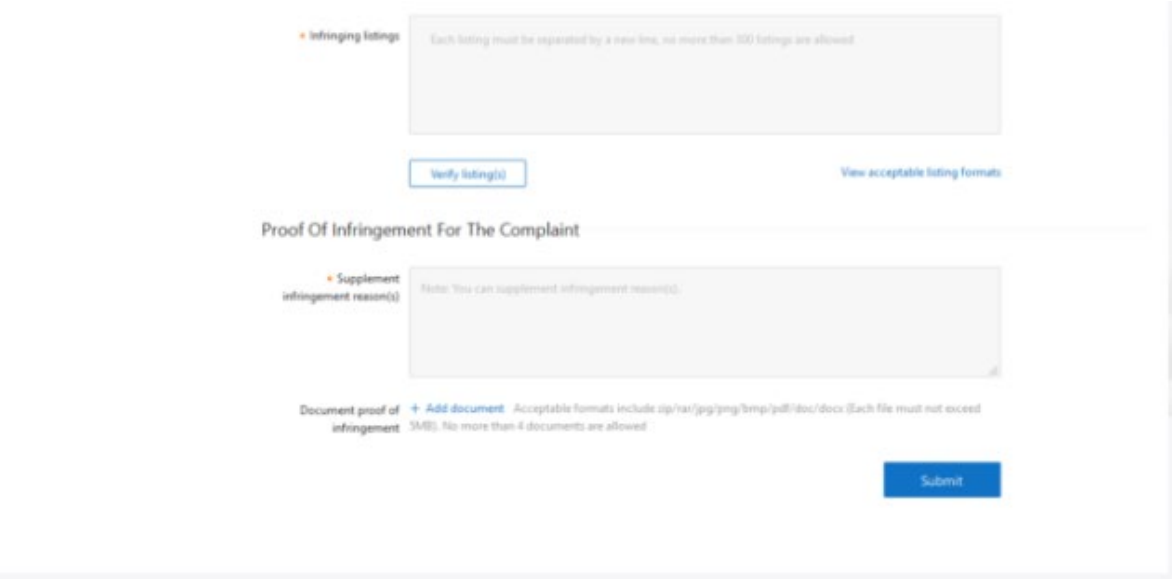
It is also possible to attach files such as copyright images or documents related to a test purchase to strengthen the claim.

At this point the user only needs to click on "Submit" and the take down request will be sent.

---

[34] For domestic platforms the rightsholder needs Chinese certificates to enforce, for Tmall Global certificates for either China or Hong Kong and for Lazada certificates registered in the country where the item is listed.

[35] Although the user can of course submit a new complaint with the correct reason code, the mistake cannot be amended, still counting as an unsuccessful takedown request as far as the good faith program is concerned.



From a brand owner perspective it is worrisome the communication by Alibaba that items for sale on Taobao may be not visible to users connected from abroad anymore. This could hinder effective enforcement from brands based outside of China. The invite to use a VPN doesn't seem to be an adequate guarantee as VPN are often blocked by the Chinese firewall[36]

2.5.3 Monitoring enforcement

Besides enforcement the IPP portal allows also to check the status of the reported listings from the 'Manage Complaints' board, nested under the 'Complaint Submission' tab in the dashboard.

Again the user will need to select one of the platforms and check the status of the complaint. As notices are subject to the seller's counternotification, in case of opposition by the seller the enforcer can check the claim under 'Check complaint details' and decide if he wants to withdraw it or keeping it firm in view of the judgement from Alibaba. In this case a reason will be needed.

The user can also reject counter notification in batches when the reason is omogeneous, still paying attention to the fact that errors will affect its participation in the good faith program.

2.6 Alibaba Web Hosting

Another service offered by Alibaba is Cloud computing. The group ranks 5th worldwide and first in China, detaining 47,7% of the domestic market share in cloud hosting in 2019 with cloud revenue up 66% year-over-years.[37] To give an idea of its leading position in China it is worth considering that the closest competitor, Tencent, detained only 14,5% of the market share in the same reference year.

Take down practice for several brand-owners has shown an increase in websites offering counterfeit items or even squatters[38] being hosted on Alibaba cloud servers. Even more worrisome is the fact that the low price of the service is increasingly attracting registrants from abroad and targeting foreign market.

---

[36] "Items listed by sellers on www.taobao.com that are available for sale only within China may no longer be viewable by users outside of China. To view all product listings on taobao.com, including those available for sale only within China, please log on to the taobao site from within China or by using the applicable VPN software." Notice on International Access to Taobao.com from 2019-11-15 available at https://ipp.alibabagroup.com/infoContent.htm?skyWindowUrl=notice/20191115/en

[37] Bavis N., "Alibaba Cloud Market Share 2019", https://www.parkmycloud.com/blog/alibaba-cloud-market-share/

[38] Squatters are individuals registering websites for ransom, to sell counterfeits or also competitors that register a website just to prevent a particular rival brand to access the market.

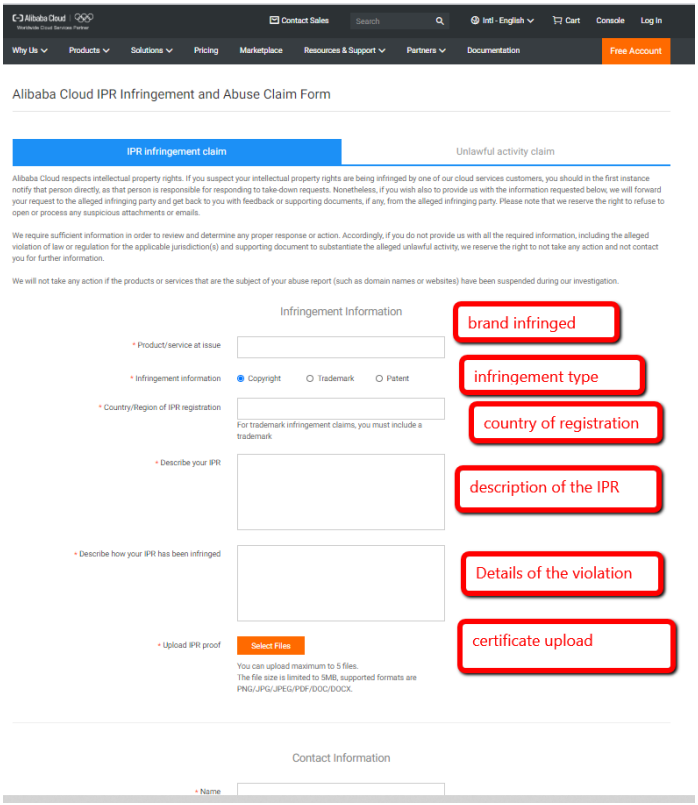
To report IP abuses users should go to https://www.alibabacloud.com/report#infringement .

The form to compile is very straightforward, and the brand owner is required to give information on the brand, the type of violation, the country were the IPR is registered and a section where to upload the certificate. There is an extra section at the bottom where to provide contact information.

Unfortunately Alibaba cloud commitments in terms of IP protection are lacking, they require to contact the infringers first and merely commit to forward the claim to the potential infringer but not to take down the domain themselves.

Take down practice has shown mixed results with different brands. When successful it takes around 5 working days.

Below a guide to compile the form.



2.7 Assessment of the IP commitment from Alibaba

The Alibaba group takes full ownership of the brand protection prerogatives that the new e-commerce law attributes to platform operators.

Overall the IPP platform represents an integrated ecosystem where the user can upload his rights, file complaints and see their status.

For some trademarks Alibaba started offering **proactive removals** across some of its platforms using keywords provided by brand owners.

Unfortunately the group does not provide full visibility on the listings that are removed in this way, making difficult for the brand owner to assess the truthfulness of the statement from Alibaba and separate it from marketing propaganda.

After the integration of **Lazada** within the group Alibaba is also actively **seeking a cooperation with big brands selling on the platform** in order to train their in house IP team on the main concerns from brand

owners. This is a good opportunity for brands to make their voice heard before the relationship is reduced to the usage of the IPP platform by sharing counterfeit indicators and minimum price lists for their products

Alibaba makes use of its discretion by **granting high rated sellers greater protection from removals**, with longer investigations of claims made against them and a dilation of the time needed to take down. [39]This is based on the assumption that new merchants with low feedback are more likely to sell counterfeits because they do not fear reputational damage.

Although this assumption is correct on a general ground it can represent a threat for brand owners because consolidated sellers are more likely to be trusted by consumers and constitute a privileged channel for the sale of counterfeits. Safeguarding the revenue from high rated sellers should not come before ensuring a uniform IP protection across the platform.

A weakness of the IPP protection from Alibaba becomes evident during single day every year,

With the IPP team being overwhelmed by take down requests that they cannot process on time before the counterfeits are sold with great damages to the brand.

If we consider that in 2019 the Alibaba Group reported a record sales of 268.4 billion yuan ($38.3 billion)[40] we understand the scope of the risk for brands.

The **Good faith program and its high standards** are also perceived by some brand owners as creating differences of treatments for different brands that do not come from the law but only from Alibaba discretional judgement and generally tend to be in favour of big enterprises.

These system weaknesses, and the consequent challenges faced by right holders in obtaining take downs, contribute to explain why in 2019 Taobao was put for the third year on a row on the United States Trade Representative's (USTR) annual list of world's most "notorious markets" for the sale of counterfeits.[41]

In its report USTR stated "Taobao remains one of the largest sources of counterfeit sales in China. Some right holders commended Taobao's improved response times and policies, but complained about the number of counterfeits offered for sale on Taobao and the lack of transparency regarding filters and other proactive anti-counterfeiting measures.."

The agency also recommended ways through which Alibaba could improve its position by simplifying processes for right holders to register and request enforcement action; making good faith takedown procedures generally available; and reducing Taobao's timelines for takedowns and issuing penalties for counterfeit sellers.

3. Tencent

This Tech giant dominates the Chinese social media market (With Wechat and QQ) and owns one of its most prominent marketplaces: Jindong and an emerging one, Pinduoduo.

There are several analogies with the rival Alibaba Group, firstly in the ambition to build an integrated ecosystem to enhance the user experience.

Tencent investments and revenues mainly revolve around media and entertainment: the company is the world's biggest gaming company and a market leader in video streaming.

Although Tencent's scope of activities range from social and entertainment to payments and investments we will cover here only the areas that are most interesting for brand owners.

---

[39] By Alibaba's admission ratings and comments on listings are among the metrics considered by the proactive scanning for infringements

[40] Cheng e., "Singles Day sales hit a record high as Chinese buyers rack up their credit card bills", 15/11/2019 available at https://www.cnbc.com/2019/11/15/singles-day-sales-hit-record-high-as-chinese-buyers-rack-up-credit-card-bills.html

[41] https://ustr.gov/sites/default/files/2019_Review_of_Notorious_Markets_for_Counterfeiting_and_Piracy.pdf

3.1 Wechat. Much more than a Social Media

The best example of Tencent's ambition to build an integrated ecosystem is WeChat (微信 in Chinese). Which became the social media of reference for Chinese Consumers in the same way Whatsapp is for the Western ones but at the same time offers much more.

While WhatsApp is merely an instant messaging platform through WeChat the user can also search and order from local restaurants, or call a taxi, access music and videos, scan QR codes, access mini programs and pay, all without leaving the app.

WeChat also built a dedicated e-payment system at its core and it constantly monitors domestic rivals for new features to imitate or simply acquire the competitors themselves in order to prevent a market loss and maintain a dominant position.

This development overshadowed also Tencent's other Social Media app, QQ which still managed to maintain a loyal user base by specializing in microblogging and desktop messaging service, while Wechat is mobile based.

Tencent may have fallen behind Alibaba in e-commerce but through Wechat and QQ maintains the leadership in social media services.

The assumption that Social Media are less of a danger for Brand Owners than Marketplaces have to be revisited because Social Media in China are often used to promote or directly sell counterfeits.

For Wechat this is done through the "Moments" sections, an area originally designed to share personal pictures and which then degenerated in a channel where counterfeiters shared pictures of their porducts availability, pricing and contact information.[42]

While marketplaces are more regulated and have public access for Wechat Moments only closed group of friends can access and look at the products so that the seller can build a network he trusts, outside the legal regulations.

The fact that the ecosystem is closed makes it difficult for law enforcers to monitor this.

Several customer simulations highlighted how many housewives and students make a living by finding consumers for companies that produce knock offs on large scale.

In this way the company itself stays protected from a legal action and can rely on easily replaceable middle men.

The punishment for these is also very lenient, a temporary block of the account that doesn't prevent them from starting again once it is over.

Even the brand protection team is short in number and they rely on brands owners to report infringements. In some cases Wechat offers to some brands the possibility to validate counterfeit claims for brand owners but the whole process is very slow and again not accompanied by serious sanctions.

Another difficulty is represented by the fact that Wechat splits Chinese and domestic users based on the telephone numbers (starting with +86 or not) and user data are stored on separate servers.

Consequently, a brand owner trying to use a western phone to investigate Chinese consumers would face yet another barrier.

3.2 RELATIONS BETWEEN WECHAT AND MARKETPLACES

The commercial evolution of Wechat is also testified by its integration with Social Media.

Tencent's leading platform – JD.com – facilitates JD sellers to set up their own WeChat store, integrated with the marketplace and providing an alternative sale channel.

[42] On the legal side also Brands can set up official accounts using the "Moment" section for promoting purposes.

The same procedure is also available for smaller platforms such as Weidian or Youzan.

Due to the increased IP protection commitments from Alibaba many counterfeiters moved their business on WeChat still characterised by a lower levels of regulation under this respect. If we sum to this the difficulty of accessing and monitoring it is easy to understand how Wechat has become a counterfeit haven for many.

Another threat for brand owners coming from Wechat is represented by **mini programs**, which are a sort of meta app that allows the users to open links with specific content while staying within the main app.

There are multiple ways to access a mini program: opening a link provided by a friend, scanning a QR code…and it is relatively easy to create them and share them among users: all features that counterfeiters are well aware of.

3.3 JD.com

Jindong is one of the biggest ecommerce companies in China and adopts a B2C model.

The platform has strong IPR protection policies in place as well as stringent vetting requirements for sellers but the burden of proof for brand owners is also heavier than in platforms belonging to the Alibaba group.

3.4 Pinduoduo

The success of Pinduoduo stems from its targeting lower tier cities respect to those that were the focus of the competition between Alibaba and JD

With fame came also more stringent regulations, especially in the field of IP, which cut its market value.

Today Pinduoduo not only provides tools to remove IP violations but also offers proactive monitoring for brands.

A potential threat is represented by the possibility for buyers to join together to make purchases, fulfilling the minimum requirements for a company to start producing a specific good with a price reflective of the economies of scale.

3.3 QQ

QQ originally was conceived as an instant messaging app and gradually expanded to offer other services.

It focuses mainly on desktop computers while Wechat took over the mobile world.

3.4 Take Downs on Wechat

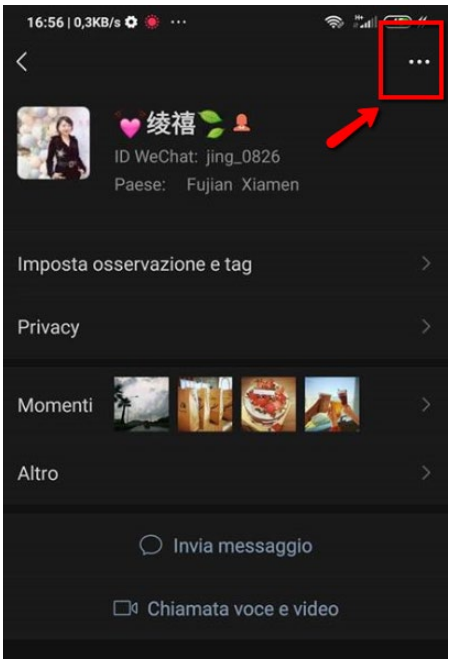
Information on how to make complaints in whatsapp can be found on the help center and the procedure is different depending on the complaint type.43

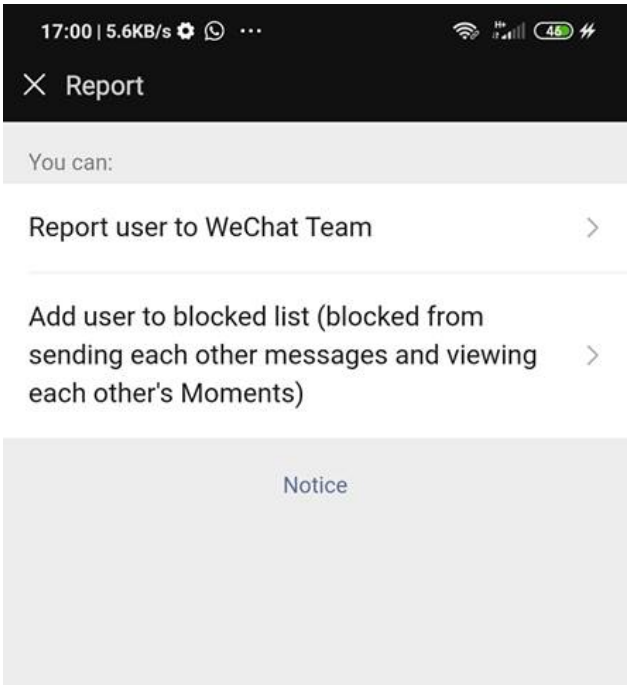
Coherently with the fact that Wechat is mobile based the complaint itself has to be completed through the mobile.

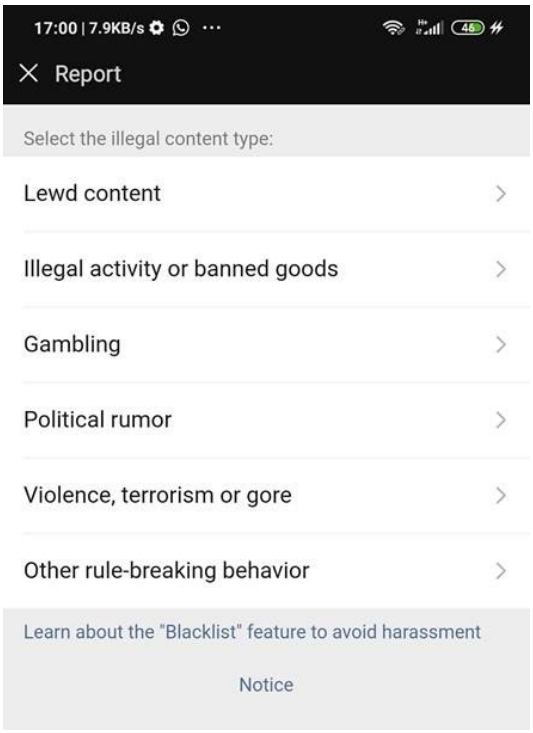
The user needs to access the Contacts section of Wechat and tap the avatar of the WeChat contact that he wants to report. At this point he needs to select "..." in the upper right, click again on Report, then select

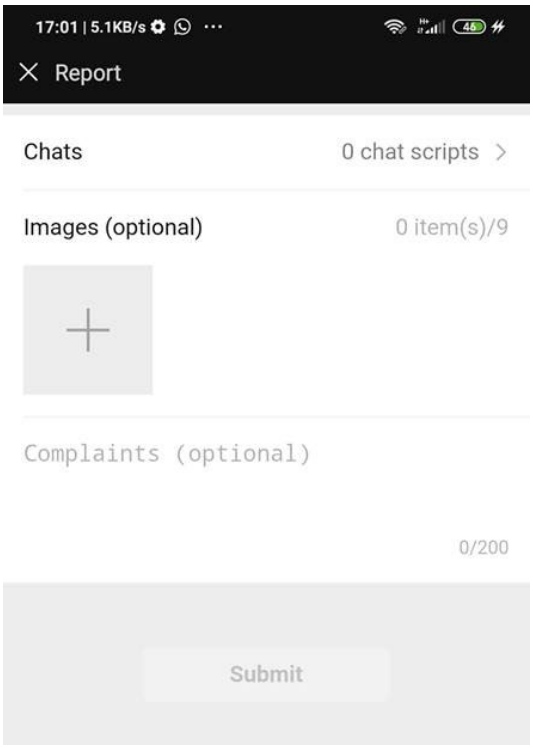
[43] The specific adress is https://help.wechat.com/cgi-bin/micromsg-bin/oshelpcenter?t=help_center/topic_detail&opcode=2&plat=android&lang=en&id=170417vMBnEB170417InAF36&Channel=

a report reason and provide the related chat scripts and images as evidence , then tap Submit to finish the report.









Providing evidence is very important as it can determine the success of the complaint. A successful complaint must include:

Essential elements:

A screenshot o of the product for sale including the user name and picture of the user(to determine the link between an user and the product being sold). For example a picture from the “Moment” section of the user

A screenshot of the conversation containing a sale attempt (price offer, link to the product from the moment section and written confirmation of the seller thet he has that product available). Again the screenshots must include the avatar of the seller and its name to be accepted as proof.

Useful elements:

The photo should be in high quality and the pictures provided should be as many as possible to help the Wechat IP team to decide on the case.

Example of screenshots:

This screenshot would not be enough because it doesn’t contain the usern name of the seller. It can be used together with another screenshot to strengthen the proof though.

This screenshot contains all the needed elements but to increase the chances of success it is better to add a HQ picture of the product (by clicking on the specific Moment) and a proof o attempted sale. We can artificially recreate them by sending a picture of the product to the seller, asking if he has it available and the price. Once the seller answers we take a screenshot of the whole conversation and send everything to Wechat.

WeChat will then handle the report and notify the result via the Official Account "WeChat Team".

The process can take up to two weeks and results in a temporary block of the account.

Due to the ease with which the seller can create a new account the measure is not resolutive.

Also the seller may put the brand owner contact in a black list and avoid adding him as friend a second time.

Wechat can also assign the brand owner the possibility to be the one validating the complaint from common users. Validation has to be done on a one on one basis and the brand owner has to deal with high volume of spam and wrongly reported incidents.

It is also contemplated the possibility to appeal against Wechat decision.

3.5 Take downs on Weibo

General take down requests on Weibo can happen by writing an email to fawu@staff.sina.com.cn.

Copyright complaints are submitted differently depending if the violation is reported under the US or Chinese Copyright Law. 44

Reporting under the US Law has to be done through the email dmca@staff.weibo.com45

In the disclaimer Weibo commits to block the repeating infringers' accounts

3.6 Take downs on JD.com

JD's IPP contemplates different remedies against Intellectual Property violations, such as Removal of the violating listings, cancellation and removal of purchases, restriction on item listing, account suspension and termination of partnership agreement.

The processing time is up to ten working days, much slower than Alibaba while the seller has the usual 2 working days to push back

Reporting has to be done through the dedicated form after successful registration.

An alternative can be using the general contact email contact@jd.com

3.7 Take downs on Pinduoduo

All takedowns in Pinduoduo have to be requested through the app.

Brand Owners can benefit from Pinduoduo's proactive take down service

4. Enforcement database

Platform	Terms of Services	Take down link
Taobao, Tmall, Tmall Global, 1688, Alibaba.com, AliExpress and Lazada		https://ipp.alibabagroup.com/
Wechat	https://weixin110.qq.com/security/readtemplate?t=fake_report/guide	
Weibo	https://service.account.weibo.com/dmca/notice	fawu@staff.sina.com.cn dmca@staff.weibo.com

[44] Detailed instructions can be found at: https://service.account.weibo.com/dmca/rightholders.
[45] Reporting under the Chinese Copyright Law must be done through the following link instead: https://service.account.weibo.com/roles/gongyue

JD	https://help.joybuy.com/help/question-312.html	https://st-en.jd.com/notice/en.html contact@jd.com
Pinduoduo		Report within the app

5. Intermediary Liability

So far we have seen remedies against infringing sellers, but what is the regime of responsibility for intermediaries in China?

Intermediaries are included in the definition of **E-commerce platform operators** from Article 9 of the Chinese Ecommerce Law.

" any legal person or unincorporated organization that provides services…for multiple parties to independently conduct transaction activities".

Being neutral with regards to the transactions (Negative requirement) is not enough to ensure intermediaries' exemption from liability, but there are a series of additional duties required by the law (Positive requirements).

In other words, neutrality, which has been historically a stronghold of the intermediaries' exemption from liability is no longer enough according to the new law which requires a set of "obligations of doing" from the intermediaries.

According to article 27 the intermediaries' responsibilities include making sure that sellers submit real information such as their identity, address, contact information, administrative license and registration, establish registration files, and verify and update them regularly.

Article 28 describes the intermediaries' disclosure obligations towards market supervision and management department but not towards other subjects with a legitimate interest (For example brand owners whose rights have been violated).

The sale of counterfeit goods can be seen as one of the cases contemplated by article 13 (commodities for which transactions are prohibited by laws) and according to article 29 in this case the intermediary shall take necessary measures in accordance with the law and report to the relevant competent authority.

Article 30 extends their duties to the prevention of illegal networks and criminal activities, and that is why platforms such as Taobao and Pinduoduo enacted systems of proactive monitoring based on sensitive keywords

Other general duties include ensuring the principles of openness, fairness, and justice, formulate platform service agreements and transaction rules and guaranteeing the quality of goods and services, protecting consumer rights, and protecting personal information.

The transaction rules should be displayed in a prominent position on their homepage and the intermediary should publicize the suspension or termination of products as a consequence of the violations of laws and regulations in accordance with platform service agreements and transaction rules. (Articles 35 and 36).

According to article 38 if the e-commerce platform operator knows or should know that the goods sold or the services provided by the seller do not meet the requirements for the protection of personal and property safety, or have other acts that infringe the legitimate rights and interests of consumers, and fail to take necessary measures, they shall bear joint and several liabilities.

For goods or services related to the life and health of consumers, if the e-commerce platform operator fails to fulfill the obligation to review the qualifications of the operators on the platform, or fails to fulfill the obligation to ensure safety to consumers, causing consumer damage, he shall bear the corresponding obligations in accordance with the law

The key provision regarding intermediaries' liability with regards to Intellectual Property violations are articles from 41 to 46.

These provisions can be further broken down between **reactive and proactive obligations**. (Articles 41-43 and 45 respectively).

First and foremost intermediaries have the obligation to establish intellectual property protection rules, strengthen cooperation with intellectual property rights holders, and protect intellectual property rights in accordance with the law.

As long as the general indications by the law is respected the implementation details are left to the intermediaries

According to Article 42 if intellectual property rights holders believe that their intellectual property rights have been infringed, they have the right to notify e-commerce platform operators to take necessary measures such as deleting, blocking, disconnecting, and terminating transactions and services. The notice should include preliminary evidence of infringement. After receiving the notice, the e-commerce platform operator shall take necessary measures in a timely manner and forward the notice to the operator on the platform (seller).

The profiles of liability are different depending on different circumstances.

If the necessary measures are not taken in time, the operator shall be jointly and severally liable for the enlarged part of the damage.

If the operator on the platform is damaged due to an error in the notification, he shall bear civil liability in accordance with the law.

If an error notice is sent maliciously and causes losses to the operators on the platform, the liability for compensation shall be doubled. (because in this case the neutrality of the intermediary is not respected).

Article 43 governs the rights of the other party in the claim (seller) and the regime of counternotifications.

After receiving the forwarded notice, the seller may submit a statement that there is no infringement to the intermediary. The statement should include preliminary evidence that there is no infringement.

After receiving the statement, the intermediary shall forward the statement to the intellectual property right holder who issued the notice and inform him that he can lodge a complaint with the relevant competent authority or file a lawsuit with the people's court.

If the intermediary does not receive a notice of complaint or lawsuit within 15 days after the transfer statement reaches the intellectual property right holder, it shall promptly terminate the measures taken.

For example on Taobao the platform remove a listings after receiving the brand owner's complaint but if the seller pushes back and there is no answer from the brand owner the product is re listed.[46]

If the previous articles draws a reactive responsibility Article 45 draws a proactive respobsibility, further extending the intermediary involvement in the transaction.

If an e-commerce platform operator knows or should have known that the operator on the platform infringes intellectual property rights, it shall take necessary measures such as deleting, blocking, disconnecting, and terminating transactions and services; if the necessary measures are not taken, it shall be jointly and severally liable with the infringer.

This article explains why several platforms belonging to Alibaba and Tencent have already taken the measure to offer proactive keyword-based monitoring to brand owners.

[46] Regarding transparency duties intermediaries shall promptly publicize the notifications, declarations and processing results received in accordance with Articles 42 and 43 of this Law.

A similar provision, outside of e-commerce, is contained in Article 4 of the Interpretations of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Network 2006,152 which states:

"*In case an Internet Service Provider providing content services is aware of the internet users' act of infringement on any other people's copyright through the network, or has been warned by the copyright owner with good evidences, but fails to take such measures as removing the infringement contents so as to eliminate the consequences of the infringement, the people's court shall, in accordance with the provisions of Article 130 of the General Principles of the Civil Law, impose contributory infringement liabilities on the Internet Service Provider and the internet users*."

Intermediary liability: case law

In case law intermediary liability for "authorizing infringement" has been based either on fault-based principles such as gross negligence, or on principles of joint or accessory liability.

An example **of fault-based secondary liability** can be observed in Music Copyright Society of China v. Netease Com., Inc. & Mobile Communications Corp.[47]

In the ruling the court held accountable the mobile operator for its negligence in its duty to

examine a work it was broadcasting, and its failure to timely interrupt the infringing work after being notified by the copyright owner.

Go East Entertainment Co. Ltd. (H.K.) v. Beijing Century Technology Co., Ltd represents instead a case of **joint or accessory liability**.

In this case, the court found the defendant, who operated the website chinamp3.com, jointly liable with the primary infringers for organizing and finalizing the various links to infringing third party sources under Article 130 of the General Principles of the Civil Law. (contributory infringement liability).[48]

The same article is the basis for the decision in Shanghai Push Sound Music & Entertainment Co., Ltd. v. Beijing FashioNow Co. Ltd.[49]

Also in this case the defendants, developers of the website and client software Kuro, were found liable, pursuant to Article 130 of the General Principles of the Civil Law, in contributory infringement.

The reason was that they intentionally assisted its users, who shared and infringed the rightholder's copyright.

The intentionality makes irrelevant the requirement of the fault for the integration of the contributory infringement liability

In other words, the fact that the plaintiff/rightholder did not send any notice to enable the defendant to take the necessary measures to remove the infringing links was considered by the court irrelevant for the purposes of the defendant's contributory liability.

What was truly essential in this case was the proven evidence of the defendant intermediary's actual knowledge of the infringement.

Defenses for intermediaries: case law

Intermediaries can use different types of defences, globally known as **Safe Harbor Defenses**.

---

[47] Music Copyright Society of China v. Netease Com., Inc. & Mobile Communications Corp., (2002)

[48] See also Article 3 of the Interpretations of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Network 2006

[49] Shanghai Push Sound Music & Entertainment Co., Ltd. v. Beijing FashioNow Co. Ltd., (2005) Er Zhong Min Chu Zi No. 13739 (Beijing No. 2 Intermediate Court, Dec. 19, 2006

- **Conduit or Passive Transmission Defense**

In Music Copyright Society of China vs. Netease Com., Inc. & Mobile Communications Corp.(2002) the Beijing Intermediate Court ruled that Mobile Communications was simply providing a passive networking service for receiving ringtones sent by Netease, without involvement with the contents of the messages transmitted, which were considered entirely under the responsibility of Netease.

This decision was later codified in Article 20 of the Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006[50].

According to this provision Internet intermediaries merely providing "automatic access" or "automatic transmission" services are not liable to compensate damage to the rightholder.

The limits of this defense is that the network service should not be involved in choosing or altering

the transmitted works, and that the latters are offered solely to its subscribers.

- **Caching Defense**

Article 21 of the Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006 provide that a network service provider that caches works, performances and audio-visual products ("materials") from another network service provider "for the purpose of elevating the efficiency of network transmission would not be liable to compensate the rightholder in damages, if the following conditions are respected:

(i) it did not alter any of the automatically cached materials

(ii) (ii) it did not affect the originating network service provider's ability to obtain information about use of the cached materials

(iii) it automatically revises, deletes or disables access to the materials where the originating network service provider does the same.

- Hosting Defense

Articles 14 to17, and 22 of the Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006 draw a safe harbor defense for Internet intermediaries providing hosting services.

The first set of articles regulates the "notice, take-down and relisting" regime.

According to the procedure the rightsholder should first send a written notice to the service provider providing his contact information, a description of the infringing materials and their web locations and the documents providing preliminary evidence that the materials are infringing and request that the service provider delete them.[51]

After receiving the take-down notice, the service provider shall "immediately delete" the

relevant materials, and at the same time, share the notice with the subscriber who published them.[52]

The subscriber can push back, requesting the relisting of the deleted materials, by supplying his contact information, the names of the materials and the documents that provide preliminary evidence that the materials are non-infringing.[53]

The service provider, on receipt of the notice, shall immediately restore the materials and transfer the relisting notice to the rightholder, who cannot further request that the materials be deleted.[54]

---

[50] Promulgated 4 years after the case

[51] Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006, Article 14

[52] Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006, Article 15

[53] Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006, Article 16

[54] Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006, Article 17

The e-commerce law recognizes broader decisional powers to the platform, that can judge over the claim of the rightholder and the counternotification, before the question is brought to Court.

Article 22 shields the intermediary from compensatory liability if:

(i) it clearly indicates that the hosting services are provided to its subscribers only, publicizes its own contact information,

(ii) does not make any alteration to the materials made available by its subscriber

(iii) it has no knowledge of and has not justifiable reason to know that the materials are infringing

(iv) it does not obtain any direct economic benefit from the provision of the materials[55]

(v) upon receiving a take-down notice from the rightholder, it acts timely to delete the materials according to the Regulations.

A proof of the fact these requirements have to be present for the exemption of liability of the intermediary is the Shanghai Xinchuan Online Co. Ltd. v. Tudou.com Co. Ltd.[56].

In this case the movie sharing platform www.tudou.com, was held liable and unable to rely on the defense from Article 22 because by uploading video under the category "popular movies" it should have known of the possibility that infringing movies would be uploaded on its website.

The negligence in monitoring and remove the infringing uploads and failure prevented the application of article 22.

Another limit is that the protection only applies if the service providers host third party materials and do not host them themselves, because in this case they would not be intermediaries in the proper sense of the word.[57]

- Referring Defense

Articles 14-17 and 23 of the Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006 grant a defence for Internet intermediaries providing referring services with the same procedure prescribed for hosting service providers.

The importance of the respect of the formal procedures emerges in EMI Group Hong Kong Limited v. Beijing Baidu Network Technology Co. Ltd., the Beijing District High Court rejected EMI's claim against the search engine Baidu because EMI's take-down notice to Baidu did not comply with the requisite formalities, and failed to specify the names of the works, their authors and the web addresses where the infringing works were found.[58]

Regarding the scope of protection Article 23 shields an intermediary offering referring services from liability only if the intermediary was not aware (and could not been aware) that the linked material was infrigning.

Hence the importance of the notification from the rightsholder[59]to claim intermediary liability.

In EMI Group Hong Kong Limited v. Beijing Baidu Network Technology Co. Ltd the Court judged that, since Search Engines rely on automated operations for referring, they should be considered as not partaking for

[55] This requirement can be disputed for online platforms that endorse or promote goods

[56] Shanghai Xinchuan Online Co. Ltd. v. Tudou.com Co. Ltd., (2007) Hu Yi Zhong Min Wu (Zhi) Chu Zi No. 129 (Shanghai No. 1 Intermediate Court, Mar. 10, 2008)

[57] Shanghai Push Sound Music & Entertainment Co., Ltd. v. Beijing Yobo Century Technology Co. Ltd., (2008) Hai Min Chu Zi No. 6939 (Beijing Haidian District People's Court, Jun. 23, 2008).

[58] EMI Group Hong Kong Limited v. Beijing Baidu Network Technology Co. Ltd., (2007) Gao Min Zhong Zi No. 593 (Beijing District High Court, Nov. 17, 2006).

[59] See Zhejiang FanYa Co. Ltd. (5fad.com) v. Beijing Yahoo! China & Alibaba Information Technology Co. Ltd., (2006) Er Zhong Min Chu Zi No. 07905 (Beijing No.2 Intermediate Court, Dec. 15, 2006).

the infringements and therefore not liable, unless is proven otherwise, with the burden of proof on the rightsholder.[60]

However a notice from the rightsholder breaks this presumption.

In Go East Entertainment Co. Ltd. (H.K.) v. Beijing Alibaba Technology Co. Ltd.[61] The rightowner only reported part of the infringing listings but the Court found still held the defendant search engine Alibaba liable for not removing all of them since the notice should have created a monitoring due diligence for the search engine and its missed activation was interpreted as favouring the infrignements and creating joint liability for Baidu.

SOURCES

- Seng D. and others, "Comparative analysis of the national approaches to the liability of internet intermediaries"
- Jung C., 24.9.2018, "How Would the New Chinese E-commerce Law Change Taobao?"

https://pandaily.com/how-would-the-new-chinese-e-commerce-law-change-taobao/

- Bavis N., "Alibaba Cloud Market Share 2019", https://www.parkmycloud.com/blog/alibaba-cloud-market-share/
- Cheng e., "Singles Day sales hit a record high as Chinese buyers rack up their credit card bills", 15/11/2019 available at https://www.cnbc.com/2019/11/15/singles-day-sales-hit-record-high-as-chinese-buyers-rack-up-credit-card-bills.html

- Peter Ganea and Thomas Pattloch, INTELLECTUAL PROPERTY LAW IN CHINA 264 (The Netherlands: Kluwer Law International, 2005)
- https://ustr.gov/sites/default/files/2019_Review_of_Notorious_Markets_for_Counterfeiting_and_Piracy.pdf

From platforms

-Notice on International Access to Taobao.com 2019-11-15

Notice of the Launch of Online Portal for Lazada 2019-06-25

Notice of Alibaba's Good-faith Takedown Mechanism Upgrade 2018-08-08

Alibaba Enhances Intellectual Property Protection Platform 2017-08-10

Alibaba, Gov't Partners in China Expand Brand Protection Efforts 2017-08-01

Alibaba Wins Civil Suit to Protect Brand's IP 2017-07-21

Alibaba's Platform Governance Team Reports Rights-Protection Progress 2017-06-19

[60] EMI Group Hong Kong Limited v. Beijing Baidu Network Technology Co. Ltd., (2007) Gao Min Zhong Zi No. 593 (Beijing District High Court, Nov. 17, 2006).

[61] Go East Entertainment Co. Ltd. (H.K.) v. Beijing Alibaba Technology Co., Ltd., (2007) Er Zhong Min Chu Zi No. 02627 (Beijing High Court, Dec. 20, 2007)

Japan

Contributor: Riccardo Ragonese (Red Points)

LEGAL FRAMEWORK FOR E-COMMERCE IN JAPAN

1. LEGISLATION

The main legal sources regulating online business in Japan are the following: Japanese Business Law including the Act on Specified Commercial Transactions, the Act against Unjustifiable Premiums and Misleading Representation, the Antique Dealing Act, the Act on Regulation of Transmission of Specified Electric Mail, the Unfair Competition Prevention Act, the Antitrust Act and intellectual property laws including the Copyright and Trademark Acts.

Additional pieces of legislation contribute to shape the regulatory framework, such as the consumer protection laws, including the Consumer Contract Law, the Act on Special Provisions to the Civil Code Concerning Electronic Consumer Contract and Electronic Acceptance Notice, the Act on Electronic Signature and Certification Business.

Finally, also the Telecommunication Business Act may be applicable depending on the contents of the consumer service provided through e-commerce. [62]

2. REGULATORY BODIES

The main bodies responsible for the regulation of e-commerce are the Ministry of Economy, Trade and Industry (METI) and the Ministry of Internal Affairs and Communications (MIC)[63].

Since September 2009 the Consumer Agency has also assumed responsibility for the aspects connected to consumer protection in e-commerce.[64]

3. JURISDICTION

There is no specific test or rule applied by the courts to determine the jurisdiction for internet-related transactions (or disputes).

This means that the Civil Procedure Act, applied to determine the jurisdiction of general transaction (or disputes), is effective also in such cases.

The rules are different if the choice of jurisdiction is internal or external respect to Japan.

Jurisdiction agreements made online by agreeing to the terms of service of a website are enforceable by virtue of applicable amendments to the Civil Procedure Act in 2005.[65]

When jurisdiction agreements appoint a court outside Japan the agreement must be made in written form at least by one party to the transaction.[66]

---

[62] Tomoya Fujimoto, Mori Hamada & Matsumoto, "Getting the Deal Through", 2010, available at: http://www.mhmjapan.com/content/files/00015374/Japan.pdf, PP. 81-85

[63] The latter is also responsible for the regulation of internet access, tariffs and charges.

[64] As a consequence of the approval by the Parliament of a bill passed on May 2009, extending the competences of the Agency

[65] Jurisdiction clauses signed prior to 1 April 2005 that appoint a court in Japan had to be in written form.

[66] As decided in the case SC, 28 November 1975 .

4. DOMAINS AND CYBERSQUATTING

To register a domain name in Japan it is necessary to apply for registration at the Japan Registry Service (JPRS), which is the body that holds the authority to confer licence to use domain names.

The licence has to be renewed every year.

Although it is possible to register a country-specific domain name without being a resident in Japan the application can be refused if the applicant does not have a contact address in Japan.[67]

Regarding brand protection the license of a domain name does not confer any additional rights but, in case such name is also used as an indication of goods or business (trade name, product name or service name) and is well known among consumers, its owner can exercise rights under the Unfair Competition Prevention Act.

Being the legitimate trademark holder allows also to claim against a 'pirate' registration of a similar domain name with the registered trademark because the use as a domain name may be considered as a use of the trademark.

5. LIABILITY: Obligations of the ecommerce sellers and intermediaries

Since there is no specific legislation governing e-commerce general provisions from other laws find their application also in this area.

One example is the Unfair Competition Act, whose Article 2.1 defines Unfair competition as

"*the act of creating confusion with another person's goods or business by using an indication of goods or business (meaning a name, trade name, trademark, markings, containers or packaging for goods belonging to a business, or any other indication of a person's goods or business; the same applies hereinafter) that is identical or similar to the another person's indication of goods or business that is well-known among consumers as belonging to that person, or by transferring, delivering, displaying for the purpose of transfer or delivery, exporting, importing or providing through a telecommunications line goods that use the same indication*"

This provision includes also the online sale of counterfeit goods, as the specificity of goods provided by means of telecommunication line is directly mentioned by the article.

Regarding the remedies that the law recognizes to brand owners they include suspension and prevention of the infringement as well as damages but they can be used against the infringer only, as **the law does not contemplate any hypothesis of intermediary liability**.

Article 3 of the Unfair Competition Act (*1) "A person whose business interests have been infringed on or are likely to be infringed on due to unfair competition may make a claim to suspend or prevent that infringement, against the person that infringed or is likely to infringe on the business interests*."

Article 36 of the Trademark Act: "*The holder of trademark right or of exclusive right to use may demand a person who is infringing or is likely to infringe the trademark right or the exclusive right to use to suspend or prevent the infringement."*

Article 112 of the Copyright Act (1970): "*The author, copyright owner, owner of print rights, performer, or owner of neighboring rights, may file a claim against a person who is infringing or who is likely to infringe the moral rights of the author, the copyright, the print rights, the moral rights of the performer, or the neighboring rights, for the cessation or prevention of such infringement."*

[67] According to the terms of service of JPDirect (the registry service conducted by JPRS)

In all these legal provisions the reference is always the primary infringer and no injunction is possible against intermediaries.[68]

Despite these general provisions there are some examples in case law that held liable intermediaries by extending to them the qualification of primary infringers.[69]

Whenever expanding the configuration as primary infringers was not possible the Japanese courts have consistently denied intermediary liability.[70]

If injunctions against intermediaries are denied also damage liability and disclosure obligations for intermediaries are limited by another law, **the Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders**.

This law broadly applies to all types of infringements, from copyright and trademark violations to defamation and privacy breaching.

In relation to damage liability Article 3 specifies:

"*When any right of others is infringed by information distribution via specified telecommunications, the specified telecommunications service provider who uses specified telecommunications facilities for said specified telecommunications (hereinafter in this paragraph referred to as a "relevant service provider") shall not be liable for any loss incurred from such infringement, unless where it is technically possible to take measures for preventing such information from being transmitted to unspecified persons and such event of infringement falls under any of the following items*"

This provision create a safe harbour environment in which intermediaries are shielded from liability for the acts of third parties who use this infrastructure for their own purposes.

Consequently Internet Service Providers (ISPs) are not responsible if their users commit actions against the law and e-commerce platforms and social media are not liable if people sell counterfeit goods through them.

The immunity is not complete and does not apply if the intermediary knew the infringement, or there is a

reasonable ground to find that it could have known the infringement.

This means that the brand owners and their representative can bring to the attention of the intermediary the violation to trigger a removal and also explains why the main ecommerce platforms have IP protection procedures in place.

Article 4 disciplines sender's identification information disclosure requests and subordinates it to a series of limits:

---

[68] On the topic an interesting reading is Ueno T., "*Liability of intermediaries in Japanese Copyright Law*" and Intellectual Property Liability of Consumers, Facilitators and Intermediaries : The
Position in Japan, by the same author, in: Christopher Heath / Anselm Kamperman Sanders (ed.) Intellectual Property Liability of Consumers, Facilitators and Intermediaries (Kluwer, 2012)

[69] The cases are the following:

- Japanese Supreme Court, 15 March 1988, 42-3 Minshū 199 [Club Cat's-Eye Case]
- IP High Court, 8 September 2010, 2115 Hanreijihō 102 [TV Break Case]
- Tokyo High Court, 31 March 2005, Case No.405 (ne) of 2004 [File Rogue Case].
- Tokyo High Court, 3 March 2005, 1893 Hanrei Jihō 126 [2-Channel Case].

[70] See:

- Osaka District Court, 20 June 2013, 2218 Hanrei Jihō 112 [Rocket News 24 Case]
- Tokyo District Court, 15 September 2016, Case No.17928 of 2015 [Retweet Case]

- The party demanding said disclosure should demonstrate that his rights were infringed by the distribution of the infringing information.
- the information of the sender is necessary for the person demanding said disclosure to exercise his or her rights to claim damages
- The intermediary must also hear the opinion of the sender of the infringing information pertaining to said demand for disclosure on whether said sender consents to the disclosure of his or her identification information, except where said provider is unable to contact said sender or where there are special circumstances.

If these provisions narrow considerably the cases in which the disclosure is allowed the fact that no penalty is contemplated where the intermediary refuses to provide such information restricts even more the scope of application.

"*The provider of disclosure-related service shall not be liable for any loss incurred by the person who demanded for said disclosure in accordance with the provisions of paragraph (1) arising from said provider's refusal of said demand, unless there is any willful act or gross negligence on the part of said provider*."

If we consider that sellers represent a profit for online marketplaces we understand how they have no incentive to disclose information unless such denial can result in gross negligence on their part.[71]

The Act on the Limitation of Liability was reviewed in 2010 and there were proposals to amend the act in consideration of several topics, such as Notices and Takedown, Three strikes policy, Reasonable measures and Monitoring obligation but eventually no action was taken.

As a consequence platforms adopted different measures in regards to brand protection, which we will examine in the following

5.5 Case Law concerning intermediary liability

Although the Japanese Copyright Act recognized the exclusive rights of copyright to the author[72] or the rightsholder as transferee of the copyright by the author[73] the liability was always considered as pertaining to the primary infringer.

The idea of an intermediary's joint liability came to consideration for the first time in 1988 in the Club Cat's Eye/Singing at a Karaoke Lounge case.

In this case the Supreme Court judged the defendant, a snack bar, jointly liable for the musical performance by its customers who had sang on the karaoke equipment and licensed tapes provided by the defendant without paying the additional license fees to the Japanese Society for Rights of Authors, Composers and Publishers (JASRAC).

The reason for this ruling was the alleged encouragement to the conduct by the staff of the bar as part of their commercial activity.

The ruling created a precedent, later know as the "Karaoke Principle" that was applied also in other similar cases.

In the Video Mates case[74], the Supreme Court applied the Karaoke principle to hold liable a karaoke equipment lessor for leasing karaoke equipment without checking if the lessee had paid the fees due to JASRAC, infringing its "reasonable duty of care.

---

[71] However there are platforms that expressely contemplate the remedy of disclosure of information such as Rakuma.(see dedicated paragraph)

[72] Japanese Copyright Act, Art. 17

[73] Japanese Copyright Act, Art. 61

[74] Supply of Karaoke Equipment for Business Use ("Video Mates" Case), 2000 (Ju) No.222 (2001) (Japanese Sup. Ct., Mar. 2, 2001

A similar judgement was rendered in the Miruku case[75], were the intermediary, again a snack bar, was considered a co-infringer with the primary defendant.

Analogue principles were applied in the File Rogue case[76], where the Internet service

provider MMO Japan Ltd, was found guilty for offering the File Rogue file sharing service, which enabled its

users to search and share unlicensed music files.

The court held that MMO Japan Ltd was or should have been aware of the nature of the files exchanged based on the titles of the songs, being therefore in the position to exercise control over their users' conduct, which they didn't. Furthermore the fact that the service, originally free, was meant to become premium reinforced the thesis of the economic interest of the intermediary in the illegal sharing.

In Rokuga Net[77], the Japanese Intellectual Property High Court held a service provider liable for providing a paid service allowing the transmission of Japanese broadcasts to overseas users via the Internet.

Conversely, in the Maneki TV case[78], the service provider was held not liable for providing a for-profit service that also involved a re-transmission abroad of Japanese broadcasts.

The difference in treatment is justified by the degree of control and management of the intermediary over the activities of the user: the provider in Rokuga Net managed the entirety of his own setup and equipment for recording and transmitting the rightholders' broadcasts, while the provider in Maneki TV required the user to purchase a piece of equipment which was owned and remotely operated by the users, and that the

provider was only entrusted with them.

The business structure of the defendant was relevant also in the Winny II case[79] , where the Osaka High Court established that the defendant's P2P software for file sharing was "value-neutral technology" and the fact that it could be used also for non-infringing purposes was not enough to create liability for the intermediary.

Only in 2001 the profiles of intermediary responsibility were codified in the Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders.

6. THE ECOMMERCE LANDSCAPE: MAIN PLAYERS

Ecommerce in Japan is characterized by the presence of foreign companies such as Amazon and Yahoo! Japan (taken over by the Chinese e-commerce giant Alibaba[80]) and autochthonous Japanese e-commerce companies, led by Rakuten, Rakuma and Mercari.

In lack of a dedicated law regulating e-commerce the regulations put in place by platforms to ensure the respect of intellectual Property assume an even greater importance.

---

[75] Japanese Society for Rights of Authors, Composers and Publishers v. Miruku Bar & Anor.,HANREI JIHO (No. 1624) 131 (27 Feb. 1997, Osaka High Ct.).

[76] 187 File Rogue, Heisei 16 (Ne) 446 (2003) (Tokyo High Ct., Mar. 31, 2005).

[77] Rokuga Net, 2005 (Ra) No.10007, 10008, 10009, 10010, 10011, 10012 (Intellectual Property High Court, Nov. 15, 2005).

[78] Maneki TV, 2006 (La) No. 10012 (Tokyo District Court, Jun. 20, 2008)

[79] Kazuo Ohtake, Two IPHC Decisions on the Infringement of Neighbouring Rights (May 2007)

[80] "Top 10 e-commerce sites in Japan 2019", available at "https://disfold.com/top-e-commerce-sites-japan/"

1. Amazon Japan

The Japanese branch of Amazon implements the same take-down procedures of the other branches, enabling intellectual property rights owners to file reports through the dedicated Report Infringement form or through the Brand Registry

This uniformity applies also to the limitations and Amazon states it does not take action in all the following cases: items marked as compatible with a certain brand, independently from their quality or the risk they may pose to the consumer, Minimum Advertised Price and Exclusive Distribution agreements.

While in most of the platforms each seller creates an individual listing, in Amazon when a detail page is created, it becomes a permanent catalog page on Amazon.com and all the sellers are nested under that page.

This means that the page will remain even if the creator's inventory sells out or if it uses official images from the brand owner.

Furthermore, Amazon specifies that when a brand owner adds a copyrighted image to a detail page, it grants Amazon and its affiliates a non-exclusive, worldwide, royalty-free, perpetual, irrevocable right to exercise all rights of publicity over the material.

The consequence is that sellers different from the brand owner can list their items under pages created by the latter or add other copyrighted images to it.

The only contemplated remedy is that if a seller adds a copyrighted image to the catalog without permission the brand owner can report it for copyright abuse, but individual sellers cannot be prevented from using the images that the brand owner himself added to the catalog.

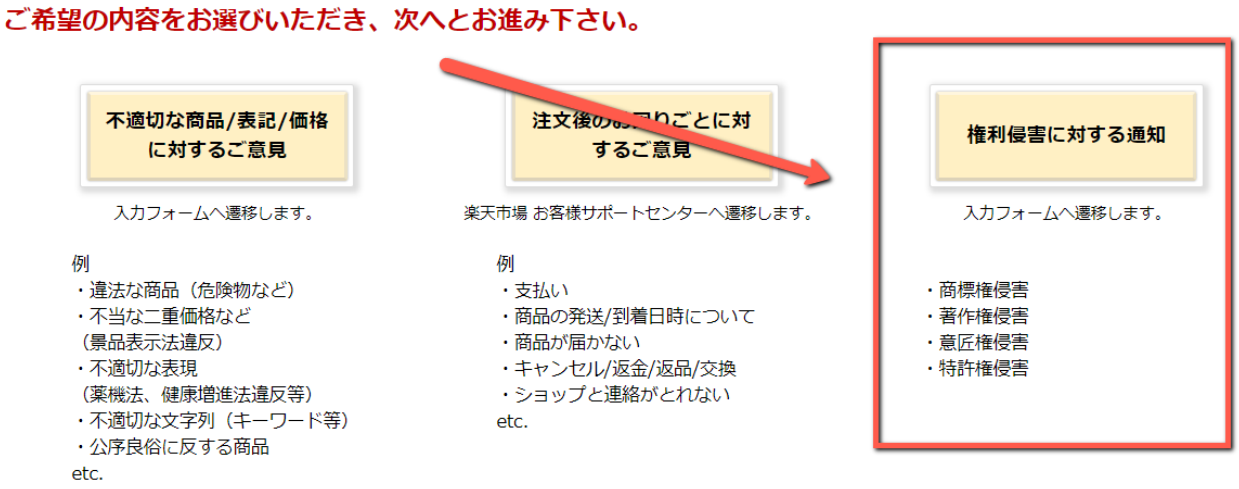
2. Rakuten

Established in 1997, Rakuten is a Japanese e-commerce and online retailing company. (B2C)

It offers a wide variety of goods, from electronics to cosmetics.

To report a violation on Rakuten the user should open the listing page and complete the dedicated form at the top right corner of the page. (不適切な商品を報告).

At this point the correct reason must be chosen (trademark, copyright, design or patent violation)



Alternatively the user can report multiple listings at the same time by filling the form available at the following url and attaching the requested documents.

https://ichiba.faq.rakuten.net/form/rightsmanagement-post

The limitations are that the complaints have to be done in Japanese and the price point alone is not accepted as a reason for removal.

This means that even when products are sold for a price that is way lower than the production cost (for example jewellery) the claimant should still add other reasons to support his complaint.

3. Rakuma

Rakuma is the C2C branch of Rakuten, established in 2014 through the merger with its former competitor Fril, and it is mobile based.

Today its url is still that of the old company: https://fril.jp/

The platform contemplates two ways to report infringements: a single " declaration-type program " for all customers to file a claim for infringement and a " registration-type program " for doing so on a regular basis.

Under the “declaration-type program every time the right holder or his representative discovers an infringing product Rakuma, he is asked to provide information and various materials to prove the infringement, and send it through the dedicated web form.

He can request either deletion or disclosure of seller information.

The petitioner can be the right holder himself (regardless if corporation or individual), an agent who can prove the delegation relationship from the right holder, or an organization that can demonstrate a similar relationship with the brand owner[81].

A registration eliminates the need to submit identity verification information each time. After the registration is completed, Rakuma will automatically recognize the request for deletion or disclosure of sender information as coming from the registered right holder.

A limit is the fact that registration is only allowed for corporatios and registration by an agent is not allowed.

Although Rakuma and Rakuten share the same ownership the first seems to have a better IP program in place and enforcement practice has shown better understanding of the reasons of the brand owners.[82]

[81] The link to the web-form is the following: https://fril.jp/info/rights_holder_inquiry/

[82] Identical cases have been judged more favourably in Rakuma.

4. Mercari

Founded in 2013 Mercari enables users to buy and sell their own products, as well as notorious brands, directly from their smartphones.

Its peculiarities are a live streaming e-commerce channel and the Mercari Now service, that allows users to receive cash instantly for their items.

The platform expanded also to the United States in 2014 and the United Kingdom in 2016

Mercari has a page dedicated to IPP commitments: https://www.mercari.com/jp/authenticity/ .

There it explains that its brand protection strategies involves 5 points:

- Proactive monitoring in cooperation and according to the guidelines of brand owners
- Hiring of professional appraisers to guarantee the authenticity of goods
- Using technology to detect frauds
- Building partnerships with investigative agencies and government agencies
- Reactive action upon notification

The platform also declares it will jointly bear the responsibility for damages borne by the purchaser of a fake product, and will compensate for the damage (the amount equivalent to the product price).

It lacks of a similar specification for the damages created to the legitimate brand owner rather than to the individual purchaser.

To report a product the user can use the specific webform for enquiries[83] or select the dedicated button on each listing by opening the item description and pressing '…'

At this point the button 'この商品を事務局に報告 needs to be pressed and the reason for reporting indicated by pressing the '事務局に報告する' button.

5. Yahoo! Shopping Japan

Yahoo! Japan Shopping is the e-commerce store of the web portal of Yahoo! Japan. The latter is owned by Soft Bank and Alibaba, and its various services are leading the Japanese digital scene.

It has an estimated monthly traffic of 85.1 Million visits.

The platform does not include a transparent description of its IPP mechanisms in the disclaimer or in the Terms of Service, only underlining their own neutrality and the contract being a matter involving the customer and seller only.

Items have been reported through the specific button in the product page.

[83] https://about.mercari.com/contact/rights-infringement/

6. Yahoo! Auctions Japan

With an estimated 135 million visits per month Yahoo! Auctions is an auctions e-commerce platform belonging to Yahoo! Japan.

Again the items needs to be reported from the product page with the additional obstacle that being products on auction the price point cannot be used as a reason for removals.

7. Amazon Japan

The Japanese branch of Amazon implements the same take-down procedures of the other branches, enabling intellectual property rights owners to file reports through the dedicated Report Infringement form or through the Brand Registry

This uniformity applies also to the limitations and Amazon states it does not take action in all the following cases: items marked as compatible with a certain brand, independently from their quality or the risk they may pose to the consumer, Minimum Advertised Price and Exclusive Distribution agreements.

While in most of the platforms each seller creates an individual listing, in Amazon when a detail page is created, it becomes a permanent catalog page on Amazon.com and all the sellers are nested under that page.

This means that the page will remain even if the creator's inventory sells out or if it uses official images from the brand owner.

Furthermore, Amazon specifies that when a brand owner adds a copyrighted image to a detail page, it grants Amazon and its affiliates a non-exclusive, worldwide, royalty-free, perpetual, irrevocable right to exercise all rights of publicity over the material.

The consequence is that sellers different from the brand owner can list their items under pages created by the latter or add other copyrighted images to it.

The only contemplated remedy is that if a seller adds a copyrighted image to the catalog without permission the brand owner can report it for copyright abuse, but individual sellers cannot be prevented from using the images that the brand owner himself added to the catalogue.

7. ENFORCEMENT DATABASE

PLATFORMS	IPP POLICY	WEB-FORMS

Amazon JP	https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=201995100	(Singular reports) https://www.amazon.co.jp/report/infringementhttps://www.amazon.co.jp/report/infringementhttps://www.amazon.co.jp/report/infringement (Multiple reports) Amazon Brand registry
Yahoo.jp	https://s.yimg.jp/images/biz_ec/pdf/provision/provision_store_revision.pdf	Report button on each listing
Yahoo Auction		Report button on each listing
Rakuten	https://www.rakuten.co.jp/doc/info/rule/ichiba_shopping.html	https://ichiba.faq.rakuten.net/form/rightsmanagement-post
Rakuma	https://fril.jp/ppip	
Mercari	https://www.mercari.com/jp/help_center/article/830/#a1	https://about.mercari.com/contact/rights-infringement/ or Report button on each listing.