Asian Journal of Law and Society, 7 (2020), pp. 345–368
doi:10.1017/als.2019.27

Internet (Un)Immunity: Where Does China Stand?

Jie (Jeanne) HUANG*
University of Sydney Law School

Abstract
This paper focuses on Internet intermediaries' civil liabilities for contents produced by third parties. By comparing Chinese law with the laws of the US and EU, it argues that the US law grants broad civil immunity to Internet intermediaries, and the EU and China restrict civil immunity to intermediaries but in different ways. This is on account of how, in the US, Internet intermediaries enjoy civil immunity as long as they do not become content providers. In the EU, aside from mere conduit intermediaries, all other intermediaries are subject to the notice-and-take-down mechanism before enjoying civil immunity. In contrast, in China, even after an intermediary properly follows the notice-and-take-down mechanism, it may still be subject to civil liability under the Chinese Consumer Law. Further, this paper argues that the policy priority for the law for Internet intermediaries varies fundamentally in the three jurisdictions. The US law for intermediaries' liability focuses on protecting freedom of speech. The EU emphasizes the protection of personal information as a fundamental human right. Contrastingly, Chinese policy priority is unclear. Consumer protection has boomed in public popularity and increasingly attracted the attentions of the legislature and judiciary in China. However, it is doubtable that the protection of consumers can provide a prevailing policy support for Chinese law in the same way as freedom of speech and the protection of personal information do under the laws of the US and the EU, respectively.

Keywords: Internet intermediary, civil liability, immunity, e-commerce, digital trade, China

1. INTRODUCTION

The Internet cannot prosper without Internet intermediaries. Although these intermediaries neither create online content nor initiate the decision to disseminate such materials, they are nonetheless vital for the transmission of online information, since they may function as Internet search engines (e.g. Google and Baidu), social media (e.g. Facebook and WeChat), and e-commerce platforms (e.g. Amazon, eBay, and Alibaba). Recent years have witnessed the adoption of starkly different law by two major international trade

* Dr Jie (Jeanne) Huang is an Associate Professor at the University of Sydney Law School. I am very grateful for the anonymous referee's comments. All errors remain to be mine. Correspondence to Jie (Jeanne) Huang, New Law Building F10, The University of Sydney, NSW, 2006 Sydney, Australia. E-mail address: jeanne.huang@sydney.edu.au. This paper was made possible partly by the University of Sydney—SJTU Research Project Grants and the China National Social Science Fund (16BFX202).

blocks in order to regulate what civil liability[1] an Internet intermediary[2] should bear for online contents created or owned by third parties. In North America, based on section 230 of the Communication Decency Act (hereinafter "CDA"), the US convinced Canada and Mexico to conclude the US-Mexico-Canada Agreement (hereinafter "USMCA") in 2018. The USMCA provides that Internet intermediaries should *not* be held civilly liable for the contents produced by a third party (hereinafter "Internet immunity").[3] Unlike the US CDA section 230, the EU E-commerce Directive divides intermediaries into three categories (mere conduit, caching, and hosting) and applies restricted immunity to intermediaries (hereinafter "restricted Internet immunity"). The restriction was expanded with the Court of Justice of the EU (hereinafter "CJEU") decision in the *Google Spain* case[4] and most recently the General Data Protection Regulation (hereinafter "GDPR") effective in 2018.[5] Both impose a high requirement for data protection and privacy in the processing of personal data within the European Economic Area (hereinafter "EEA") and any enterprise (including Internet intermediaries) that processes the personal information of data subjects within the EEA.

The North American and the European trade blocks are competing in shaping global digital trade law, including the establishment of global e-commerce rules at the World Trade Organization.[6] Other countries find themselves caught in a global law-making battle in which the USMCA demands Internet immunity, whilst the EU restricts it.[7]

In this battle, where does China stand? It is estimated that, in 2019, China will be the top global e-commerce market, with e-commerce sales more than three times greater than the US, estimated to be positioned just below China at second.[8] As such, Chinese views on the liability of Internet intermediaries for contents produced by third parties are critically important for the development of global law for digital trade. Indeed, 2018 was also a landmark year for Chinese law on digital trade: China's E-commerce Law was enacted. In this context, this paper hopes to add to existing literature: it compares Chinese law on intermediaries with those of the US and the EU. It argues that the US law grants broad civil immunity to Internet intermediaries, and the EU and China restrict civil immunity to intermediaries but in different ways. This is on account of how, in the US, Internet intermediaries enjoy civil immunity as long as they do not become content providers. In the EU, aside from mere conduit intermediaries, all other intermediaries are subject to the notice-and-take-down mechanism

1. This paper does not discuss intellectual-property law so it does not cover civil liability of intellectual-property infringements.

2. For the definition of "Internet intermediary" in this paper, see Section 2.

3. Art. 19.17 of USMCA. For the text of USMCA, see https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between (accessed 7 November 2019).

4. C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, ECLI:EU:C:2014:317.

5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) [2016] OJ L119/1.

6. See World Trade Organization (2019).

7. Whether Internet intermediaries should bear liability for contents produced by their users is also a thorny issue for many other countries. For example, in Australia, commentators describe that "[t]here are conflicting authorities both within and between separate bodies of law that impose different standards of responsibility on online intermediaries." Pappalardo and Suzor (2018), p. 471.

8. eMarketer.com (2019).

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

before enjoying civil immunity. In contrast, in China, all intermediaries are subject to the notice-and-take-down mechanism but, even after an intermediary properly follows the notice-and-take-down mechanism, it may still be subject to civil liability under the Chinese Consumer Law. Further, this paper argues that the policy priority for the law for Internet intermediaries varies fundamentally in the three jurisdictions. The US law for intermediaries' liability focuses on protecting freedom of speech under the First and Fourteenth Amendments of the US Constitution.[9] The EU emphasizes the protection of personal information as a fundamental human right. Contrastingly, Chinese policy priority is unclear. Though consumer protection has boomed in public popularity and increasingly attracted the attentions of the legislature and judiciary in China, it is doubtable that the protection of consumers can provide a prevailing policy support for Chinese law in the same way as freedom of speech and the protection of personal information do under the laws of the US and the EU.

In addition to this introduction, this paper has five parts. The first part defines Internet intermediaries. The second part explores Internet immunity under the US law, arguing that US law does not create a notice-and-take-down mechanism, but rather broadly exempts intermediaries from civil liability arising from contents produced by third parties. The third part discusses the EU law. It posits that the law of the EU creates restricted Internet immunity by the notice-and-take-down mechanism. The law of the EU highlights the protection of personal information as a fundamental human right. The fourth part focuses on Chinese law. Specifically, it contends that Chinese law also restricts the civil immunity that intermediaries can enjoy but with significant differences compared with the EU. The fifth part concludes the paper.

2. INTERNET INTERMEDIARY

In this paper, "Internet intermediary" refers to online services that do not produce or own online content. Intermediaries may function as Internet-access platforms, service providers, data-processing or web-hosting providers, such as domain-name registrars, Internet search engines, e-commerce platforms that do not take title to the goods being sold, e-commerce payment systems, and participatory media that do not create or own their content being published or broadcasted.[10] Intermediaries should be distinguished from information content providers; indeed, they are mutually exclusive.

In the US, "Internet intermediaries" denote interactive computer services under the US's CDA § 230. "Interactive computer service" is defined as

> any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.[11]

9. U.S. CONST. amend. I and IV.
10. OECD.org (2010), p. 9.
11. (f)(2) of 47 U.S. Code § 230.

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

This definition under CDA § 230 resonates with the definition of "Interactive computer service" in the USMACA.[12] Interactive computer service providers (i.e. intermediary) and information content providers are mutually exclusive.[13] The latter refers to a person or entity that creates or develops, wholly or partly, information provided through the Internet or another interactive computer service.[14]

As for the EU, the law divides Internet intermediaries into three categories: mere conduit, caching, and hosting information society services.[15] "Information society services" are broadly defined as including the provision of an online platform to sell goods and services owned by a third party; offering online information or commercial communications; allowing the search, access, and retrieval of data; transmitting information via a communication network; providing access to a communication network; or hosting information provided by a recipient of the service.[16]

Conversely, Chinese law lacks a uniform definition of "intermediaries." For instance, Article 22.2 of the Administrative Measures for Online Trading defines "third-party trading platform" as the information network systems providing webpage space, virtual business places, trading rules, match-making, information release, and other relevant services for both or all trading parties in online commodity-trading activities, which are available for both or all trading parties to independently conduct trading activities. This definition excludes intermediaries providing network access, server hosting, virtual-space lease, website and webpage design, and production, etc. The Chinese E-commerce Law provides that "e-commerce platform operators" signify legal persons or unincorporated associations that provide two or more parties in e-commerce transactions with services such as network business premises, deal making, and information release for the aforesaid parties to carry out transactions independently.[17] It is unclear whether this definition applies to Internet search engines, e-commerce payment systems, and social media. For example, many dealers sell products on Chinese social media WeChat. Could WeChat be considered as an "e-commerce platform operator"? The answer should be in the affirmative, as WeChat offers network business premises that facilitate deal making between customers and persons undertaking online business (i.e. Internet content providers).

Like the US's CDA § 230, Chinese law also distinguishes intermediaries from information content providers. Article 4 of the Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information Networks (hereinafter "SPC

12. USMCA Art. 19.1 defines "interactive computer service" as "a system or service that provides or enables electronic access by multiple users to a computer server."

13. Stewart (2013), pp. 239–40.

14. (f)(4) of 47 U.S. Code § 230 and Art. 19.1 of USMCA.

15. Arts 12–15 of EU E-commerce Directive.

16. Information society services do not include TV or radio broadcasting; the use of electronic mail or equivalent individual communications, e.g. by natural persons acting outside their trade, business, or profession, including their use for the conclusion of contracts between such persons, is not an information society service the contractual relationship between an employee and his employer is not an information society service; activities that, by their very nature, cannot be carried out at a distance and by electronic means, such as the statutory auditing of company accounts or medical advice requiring the physical examination of a patient, are not information society services. Para. 18, Recitals of EU E-commerce Directive.

17. Art. 9 of Chinese E-commerce Law.

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

Provisions on Right of Dissemination") provides that, if the network service provider is able to produce evidence proving that it only provided automatic connections; automatic transmissions; information storage space; search, link, file-sharing technology; or other network services that do not contribute to an infringement, the network service provider should not be liable for the infringement caused by a third party using its service.[18] However, if a network service provider has provided any work, performance, or audio- or video-recording jointly with others by means such as co-operation, constituting a joint infringement, the People's Court shall hold the network service provider jointly and severally liable.[19] Therefore, "intermediary" denotes the service that provides automatic connections; automatic transmissions; information storage space; search, link, file-sharing technology; or other network services.

As a conclusion, the key feature of Internet intermediaries in the US, EU, and China is this: the intermediaries do not produce or own online content and they are not the content providers.

3. THE US: INTERNET IMMUNITY

Content providers, either offline or online, should be responsible for the materials they publish. For example, in *New York Times Co. v. Sullivan*, the Supreme Court of the US held that newspapers and other content providers would be liable for defamation if they were guilty of "actual malice" when publishing false statements about public officials.[20] However, unlike content providers, Internet intermediaries are immune from civil liabilities derived from the contents produced by a third party as long as they do not become a content provider. This is the so-called "Internet immunity," providing protection to Internet intermediaries—but not for content providers.

US courts use the "material contribution" test to determine whether an Internet intermediary exercises a content provider's editorial functions.[21] A material contribution requires more than "merely taking action that is necessary to the display of allegedly illegal content" produced by a third party.[22] For example, in *Fair Housing Council of San Fernando Valley v. Roommates.com*, the US Court of Appeals for the Ninth Circuit held that Roommates.com materially contributed to the illegality of the content because it not only required users to enter characteristics and preferences such as age, race, sex, and sexual orientation as a condition of using its website, but also designed its website to hide listings from certain users based on these protected characteristics.[23] Maintaining rights to edit, publish, or remove

18. Art. 4 of Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information Networks (hereinafter "SPC Provisions on Right of Dissemination").

19. *Ibid*.

20. *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964). "Actual malice" means "knowledge that the [publications] are false or in reckless disregard of their truth or falsity." This ruling was extended to public figures in *Curtis Publishing Co. v. Butts*, 388 U.S. 130 (1967).

21. "[A] website helps to develop unlawful content, and thus falls within § 230 (f)(3), if it contributes materially to the alleged illegality of the conduct." *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008), 1168.

22. *Jones v. Dirty World Entertainment Recordings LLC*, 755 F.3d 398, 410 (6th Cir. 2014).

23. *Fair Housing Council of San Fernando Valley*, 521 F.3d 1157 (9th Cir. 2008), 1169.

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

contents produced by a third party will not render an intermediary a content provider.[24] A licensing agreement between an intermediary and a content provider is also inadequate in transforming the former into the latter if it cannot show that the intermediary had a role in writing or editing the allegedly defamatory material.[25]

3.1 No Notice-and-Take-Down Mechanism

Internet immunity is provided by the infamous CDA § 230. In the 1990s, the US Congress recognized that intermediaries functioned as fora for diversified information exchange and possessed a great degree of control over the information that they received and transmitted online.[26] Hoping that Internet intermediaries would flourish with minimum government regulation so as to benefit all Americans, the US Congress enacted CDA § 230.[27] CDA § 230 has been praised as "the most important law protecting Internet speech."[28] Its underlying policy is to promote the continued development of the Internet, preserve the vibrant and competitive free market, maximize user control over online information, remove disincentives for blocking and filtering objectionable or inappropriate online material, and ensure the vigorous enforcement of federal criminal laws.[29]

The most important feature of CDA § 230 is (c), titled as protection for "Good Samaritan" blocking and screening of offensive material. It has two provisions. § 230 (c)(1) provides that Internet intermediaries retain civil immunity so long as they do not become "information content providers" (i.e. publishers or speakers) who are responsible, in whole or in part, for the creation or development of information provided through the Internet.[30] CDA § 230 was enacted in part to respond to *Stratton Oakmont, Inc. v. Prodigy Servs. Co*., where the New York Supreme Court held that an Internet intermediary was liable for defamation related to a message produced by a third party on its message board because it had removed other user postings from its message boards and advertised itself as family-friendly.[31] However, the scope of § 230 (c)(1) is not limited to defamation cases.[32] It has been applied to cases violating anti-discrimination laws[33]; fraud, negligent misrepresentation, and ordinary negligence[34]; false light[35]; and negligent publication of advertisements that cause harm to

24. *Ben Ezra, Weinstein, and Co., Inc., v. America Online Inc*., 206 F.3d 980,985 (10th Cir. 2000). In *Schneider v. Amazon.com*, 31 P.3d 37 (Wash.Ct.App.2001), the Washington Court of Appeals held that Amazon was not a content provider because it reserved the right to edit book reviews submitted by users and remove or refuse to post reviews that did not comply with its internal guidelines, 31 P.3d 37, 42-43 (Wash.Ct.App.2001).

25. *Blumenthal v. Drudge*, 992 F. Supp. 44, 50 (D.D.C. 1998).

26. 47 U.S. Code § 230 (a).

27. 47 U.S. Code § 230.

28. Electronic Frontier Foundation.org (2019). This law has also been described as "the law that gave us the modern Internet," the "most important law in tech," and "the law that makes the Internet go." See Khanna (2013); Zara (2017); Letter from Josh King, CEO, Avvo, to Honourable Tani Cantil-Sakauye, Chief Justice, Supreme Court of the State of California (10 August 2016).

29. 47 U.S. Code § 230 (d).

30. *Ibid*., (c).

31. *Stratton Oakmont, Inc. v. Prodigy Servs. Co*., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

32. *Barnes v. Yahoo!, Inc*. NO. 05-36189 D.C. No. CV-05-00926-AA.

33. E.g. *Fair Housing Council of San Fernando Valley*, 521 F.3d 1157 (9th Cir. 2008).

34. E.g. *Doe v. MySpace, Inc*., 528 F.3d 413 (5th Cir. 2008), cert. denied, 129 S. Ct. 600.

35. E.g. *Flowers v. Carville*, 310 F.3d 1118 (9th Cir. 2002).

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

third parties,[36] to name a few. As such, if the duty that the plaintiff alleges an interactive computer service violated derives from the defendant's status or conduct as a "publisher or speaker," CDA § 230 (c)(1) precludes liability.[37]

§ 230 (c)(2) exempts the civil liability of a provider or user of an interactive computer service from taking any voluntary action in good faith to restrict or provide technical means to restrict the availability of offensive online material.[38] § 230 (c)(2) applies to any provider of an interactive computer service, and not merely to those whom subsection (c)(1) already protects.[39] For example, in *Zango v. Kaspersky*, the Ninth Circuit Court of Appeals applies § 230 (c)(2) to vendors of anti-spam, anti-virus, and anti-malware services, and provided them with wide-ranging protection.[40]

"[T]he most important § 230 ruling today" is *Zeran v. Am. Online, Inc*.[41] *Zeran* held that § 230 aims to preclude tort-based lawsuits against Internet intermediaries for the purpose of promoting freedom of speech in "the new and burgeoning Internet medium."[42] The US Court of Appeals for the Fourth Circuit concludes that, if notice-based liability is imposed, intermediaries would have to conduct ceaseless choices of suppressing controversial speech or sustaining prohibitive liability. This is directly contrary to the statutory purposes of § 230.[43]

Indeed, whilst *Zeran* concerns torts, *Schneider v. Amazon.com, Inc*. demonstrates that CDA § 230 immunity also applies to contractual disputes.[44] Amazon.com allows third-party visitors to post comments related to publications sold on its website, provided that the postings follow Amazon's guidelines. Visitors are informed that "any review in violation of the guidelines may not be posted." The plaintiff's book was sold on Amazon and at least one posting in relation to the plaintiff's book violated Amazon's guidelines. The plaintiff brought the violation to Amazon's attention and Amazon's representative allegedly promised to remove the postings within one or two business days. However, Amazon failed to do so and the plaintiff brought the action. The Court of Appeals at the State of Washington held that the immunity under CDA § 230 requires three elements: (1) the defendant must be a provider or user of an "interactive computer service"; (2) the asserted claims must demonstrate the defendant as a publisher or speaker of information; (3) the information must be provided by another "information content provider."[45] The Court of Appeals held that, although Amazon maintained the right to edit or remove the posting, the information was provided by a third party. The plaintiff sought to recover damages arising from

36. E.g. *Braun v. Soldier of Fortune Magazine, Inc*., 968 F.2d 1110 (11th Cir. 1992).

37. *Barnes*, NO. 05-36189 D.C. No. CV-05-00926-AA.

38. 47 U.S. Code § 230 (c)(2).

39. *Barnes*, NO. 05-36189 D.C. No. CV-05-00926-AA.

40. *Zango, Inc. v. Kaspersky Lab, Inc*., 568 F.3D 1169 (9th Cir. 2009).

41. Goldman (2017), p. 3.

42. *Zeran v. Am. Online, Inc*., 129 F.3d 327, 330 (1997). This case concerned messages posted on an American Online (AOL) bulletin board. The messages advertised t-shirts with offensive language related to the bombing of the Oklahoma City federal building. Interested buyers were to call Zeran's phone number posted on the bulletin board. Zeran received a staggering number of phone calls including death threats.

43. *Zeran*, 129 F.3d 327, 333 (1997).

44. *Schneider*, 31 P.3d 37 (Wash.Ct.App.2001).

45. *Ibid*.

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

Amazon's misrepresentations and its failure to remove the offensive posting. However, the court rejected this claim, holding that

> assuming [that the plaintiff] could prove existence of an enforceable promise to remove the comments, [his] claim is based entirely on the purported breach—failure to remove the posting—which is an exercise of editorial discretion. This is the activity the statute [CDA § 230] seeks to protect.[46]

In conclusion, CDA § 230 bars lawsuits that seek to hold a service provider liable for its exercise of a publisher's traditional editorial functions including deciding where to publish, withdraw, postpone, or alter content.[47]

3.2 Emphasize Free Flow of Information

The broad Internet immunity created by CDA § 230 is controversial.[48] However, imposing restrictions on CDA § 230 is difficult, as protecting the free flow of information under CDA § 230 derives from the freedom of speech contained in the First and the Fourteenth Amendments of the US Constitution. Thus far, the most successful restriction on CDA § 230 surrounds online information related to sex trafficking. In 2017, the US Congress passed the Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (hereinafter "FOSTA").[49] FOSTA creates an exception to CDA § 230: it holds interactive computer service providers liable for third-party content "that unlawfully promote[s] or facilitate[s] prostitution and websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims."[50] Due to the wide appreciation of freedom of information in the US, FOSTA has been met with mixed responses.[51] Advocators, such as trafficking victims and survivors, welcome this exception.[52] This was accompanied by the support of big Internet companies such as Google and Facebook.[53] Conversely, some opponents criticize FOSTA on the persuasion that it would negate Internet immunity in rendering § 230 litigation less predictable and more expensive as the courts have to perform longer factual inquires.[54] Others argue that it may violate the First Amendment and the Constitution's *ex post facto* clause.[55]

In November 2018, the US, Canada, and Mexico signed the USMCA.[56] The USMCA's Article 19.17.2 provides that

---

46. *Ibid*.

47. *Ibid*.

48. Bluebond (2014), pp. 679–710.

49. Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (FOSTA), H.R.1865 (115th Cong. 2017-18).

50. Congress.gov (2017–18).

51. Kozak (2018).

52. Cecil (2014), pp. 2514–55; Jackman (2018).

53. Kozak, *supra* note 51; Reason.com (2018).

54. Goldman (2019).

55. For whether FOSTA violates the *ex post facto* clause of the US Constitution, see Honorable Ann Wagner, "Ex Post Facto Implications of the Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (H.R.1865), as Passed by the House of Representatives," Congressional Research Service, 7 March 2018.

56. Art. 19.17 of USMCA. For the text of USMCA, see https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between (accessed 7 November 2019).

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

> no Party shall adopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by the service, except to the extent the supplier or user has, in whole or in part, created, or developed the information.[57]

Article 19.17.3 offers immunity to intermediaries for their good-faith action in restricting access to harmful or objectionable contents produced by third parties. According to Article 19.17.4, the Internet immunity should not apply to intellectual-property infringement and criminal-law issues. Therefore, Article 19.17 is substantially similar to CDA § 230.[58]

Article 19.17 is subject to Article 32.1 (General Exceptions) of the USMCA that, among other things, provides an exception for measures necessary to protect public morals pursuant to paragraph (a) of Article XIV of the WTO General Agreement on Trade in Services. Domestic measures necessary to protect against online sex trafficking, sexual exploitation of children, and prostitution—such as FOSTA—are considered necessary to protect public morals.[59] If the USMCA is ratified, the broad Internet immunity will extend to Mexico and Canada.[60] Consequently, a digital market featuring free flow of information is likely to be formed among the US, Mexico, and Canada.

4. THE EU: RESTRICTED INTERNET IMMUNITY

Dissimilarly to the US, the EU applies restricted Internet immunity to intermediaries; intermediaries in the EU do not enjoy the broad civil immunities like their US counterparts. Instead, only when certain requirements (e.g. the notice-and-take-down mechanism) are fulfilled can they enjoy civil immunity to contents produced by third parties. The civil immunity based on meeting the notice-and-take-down mechanism does not apply to content providers regardless of whether they publish online or offline.[61] Also different from the US's spotlight on the free flow of information, the law of the EU imposes a higher obligation on intermediaries to protect personal information. This is because protecting personal information is considered a fundamental human right under the European Convention on Human Rights and Charter of Fundamental Rights of the EU.[62] The EU E-commerce Directive[63] and GDPR are the key EU laws regulating Internet intermediaries' liability for the contents produced by third parties.

57. Art. 19.17(2) of USMCA.

58. Ballard Spahr LLP (2018).

59. Annex 19 A of USMCA.

60. Mexico ratified the USMCA in 2019; Office of the United States Trade Representative.gov (2018).

61. Media Legal Defence Initiative.org (2015), pp. 13. 20–4, 56.

62. The European Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights, effective in 1953; for an official text, see https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c= (accessed 7 November 2019). Charter of Fundamental Rights of the European Union, 2000 O.J C 364/10: a constitutional document of the EU. Art. 8.1 contains an explicit right to data protection, indicating: "[e]veryone has the right to the protection of personal data."

63. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (hereinafter "the EU E-commerce Directive").

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

4.1 Different Notice-and-Take-Down Mechanisms

The EU E-commerce Directive divides intermediaries into three categories and offers different "notice-and-take-down mechanisms" (namely, safe-harbour rules) to protect them from civil liability arising from contents produced by third parties.[64]

The first category includes intermediaries who provide "mere conduit" services, whereby an intermediary only transmits information provided by a recipient of the service or provides access to a communication network.[65] For example, this category would apply where the information transmitted is automatically, intermediately, and transiently stored by the intermediary for the sole purpose of transmission, and only for a period reasonably necessary for the transmission. The "mere conduit" intermediary is not liable for the information transmitted if the intermediary does not initiate the transmission, does not select the receiver of the transmission, and does not select or modify the information contained in the transmission.[66]

The second category addresses intermediaries who conduct "caching."[67] Here, there are four differences between "mere conduit" and "caching." First, unlike "mere conduit," "caching" does not concern the provision of access to a communication network. Second, "caching" allows the temporary storage of information for the sole purpose of a more efficient onward transmission of information to other recipients of the service upon their request, while "mere conduit" intermediaries do not have storage services.[68] Third, the "caching" intermediary is allowed to update the information, while the "mere conduit" intermediary is not. Fourth, the "caching" intermediary is immune from liability associated with automatic, intermediate, and temporary storage of information subject to a "notice-and-take-down" scheme: the intermediary should act expeditiously to remove or disable access to the information once it has actual knowledge of the fact that the information has been removed from the network, access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement. Therefore, it is evident that the conditions to be immune from liability of third-party contents differ between "mere conduit" and "caching" intermediaries.

The third category governs an intermediary "hosting" information provided by a third party.[69] The "hosting" intermediary should be immune from liability associated with the information stored on condition that they do not have actual knowledge of any illegal activity or information, or the provider acts expeditiously to remove or disable access to the information upon obtaining such knowledge.[70] Therefore, the "notice-and-take-down" mechanism for the "caching" intermediary is different from that of the "hosting" intermediary. Namely, the

64. See Opinion of Advocate General Szpunar, Case C-484/14, *McFadden v. Sony Music Entm't Ger. GmbH*, 2016 E.C.R. 170, ¶ 64 (noting that immunity extends to "all forms of liability for unlawful acts of any kind, and thus to liability under criminal law, administrative law and civil law").

65. Art. 12 of EU E-commerce Directive.

66. *Ibid*.

67. Art. 13 of EU E-commerce Directive.

68. While storing information, a caching intermediary (1) must not modify the information, (2) must comply with the conditions on access to the information, (3) the rules regarding the updating of the information according to widely adopted industry standards, and (4) must not interfere with the lawful use of technology to obtain data to use the information; *ibid*.

69. Art. 14 of EU E-commerce Directive.

70. *Ibid*.

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

"caching" intermediary is not allowed to determine the legality of the information, while the "hosting" intermediary may do so.

For intermediaries in the second and the third categories, the "notice-and-take-down" mechanism will be triggered until the intermediary has "knowledge of illegal activity or information" produced by a third party.[71] Allegations of illegality should be sufficiently precise or adequately substantiated—otherwise an intermediary has no obligation to remove the alleged information.[72] Moreover, intermediaries have no "general obligation to monitor" or police users' online expression[73]; nor are intermediaries obliged to actively seek facts or circumstances that may indicate illegal activities.[74] This is because monitoring requirements may lead to overcautious erroneous removal of lawful speech. Similar to CDA § 230, the underlying policy of the E-commerce Directive is to encourage industry self-regulation, safeguard the public's general interest in the free flow of information, and protect the freedom of speech of Internet users.

4.2 Highlight Personal Information Protection

In the E-commerce Directive, allegations of illegality are required for the notice-and-take-down mechanism. However, the *Google Spain* case decided by CJEU in 2014 establishes the right to be forgotten, which requires an intermediary to remove personal information that is legally produced by a third party. Implemented in 2018, the GDPR further expands the intermediary's monitor duty, invoking a severe penalty to incentivize them to remove personal information produced by third parties.

The *Google Spain* case concerned a Spanish man, Mario Costeja González, whose property was auctioned because he did not pay debts on time in 1998.[75] A Spanish newspaper published a legally mandated announcement of the auction, including Mr Costeja's name. This announcement was made available online when the newspaper digitized its archives ten years later.[76] When Mr Costeja's name was searched using the Google engine, the announcement topped the results.[77] Mr Costeja complained that he had since resolved his financial problems.[78] He applied to the Spanish data-protection agency and successfully obtained an order requiring Google Spain and its parent company, Google US, to remove the auction announcement from Google's search results.[79] Google appealed. Google US argued that the Data Protection Directive (the predecessor of the GDPR) should not be applied. The CJEU disagreed and applied the Data Protection Directive to Google. It found that Google was the controller of the auction announcement because of its indexing function.[80] The court found that the Google search result established "a more or less detailed profile of the data

71. Art. 14 of EU E-commerce Directive.

72. Case C-324/09, *L'Oréal SA v. eBay Int'l AG*, 2011 E.C.R. I-6011, ¶ 122.

73. Art. 15.1 of EU E-commerce Directive. But the exact parameters of the prohibited "general" monitoring obligation is disputed; see Keller (2018), p. 341.

74. Art. 15 of EU E-commerce Directive.

75. Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.R. 317, ¶ 14.

76. Peguera (2016) pp. 507, 523.

77. *Ibid*.

78. *Ibid*.

79. *Ibid*., pp. 523–4.

80. *Google Spain SL*, 2014 E.C.R. 317, ¶ 1.

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

subject."[81] This contrasted with the Spanish newspaper that digitalized the announcement and was subject to different obligations under the Data Protection Directive.[82] The court required Google to delist the URL for the auction announcement in its search results—even if the publication by the newspaper itself was lawful.[83] Therefore, unlike the E-commerce Directive,[84] according to *Google Spain*, the public's general interest in information should not outweigh the importance of personal data protection "as a rule."[85]

Google Spain leaves two main questions unanswered. First, what are the criteria and procedures to delist a URL? The CJEU requires Google and other intermediaries to remove data that are inaccurate or "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing," taking into account public-interest factors including the individual's role in public life.[86] Evidently, this guidance is ambiguous and contains no substantive and procedural details. Google refers to Article 29 of the Working Party's guidelines[87] and develops its own criteria and procedure from there.[88] After *Google Spain*, Google received 834,733 requests to delist, and subsequently delisted 3,281,701 URLs up to August 2019.[89] Nevertheless, Google is still hauled into courts due to jurisdiction conflicts and disputes on the transparency of removal.[90] Second, *Google Spain* does not discuss the freedom of speech of content publishers. When a URL is delisted from powerful search agencies, even if it still exists online, there will be far fewer chances that it can located by other Internet users.[91] However, when Google and other intermediaries decide to remove a URL from their search results, the URL has no recourse to a regulatory agency or court to challenge the removal and protect their right to the freedom of speech.[92]

GDPR came into effect in 2018. It follows *Google Spain*, firmly establishing that a data subject has the right to erasure (i.e. "right to be forgotten").[93] According to the GDPR, a data subject shall have the right to have a data controller erase his or her personal data without undue delay; indeed, the controller is obliged to do so under one of the following grounds.[94]

81. *Ibid*., ¶ 37.

82. *Ibid*., ¶¶ 82, 85–88.

83. *Ibid*., ¶ 88.

84. E-commerce Directive is implemented by Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico [Law on Information Society and Electronic Commerce Services], Arts 14–17 (B.O.E. 2002, 34) (Spain).

85. Kuner (2015), p. 97.

86. *Google Spain SL*, 2014 E.C.R. 317, ¶¶ 92, 94.

87. Art. 29 Working Party, https://ec.europa.eu/newsroom/article29/news-overview.cfm (accessed 7 November 2019).

88. Criteria includes—but not limited to—"whether the content relates to the requester's professional life, a past crime, political office, position in public life, or whether the content is self-authored content, consists of government documents, or is journalistic in nature." On delisting URLs from Google search for privacy, see Transparencyreport.google.com (2019).

89. *Ibid*. Pages are only delisted from results in response to queries that relate to an individual's name.

90. Keller, *supra* note 73, p. 327.

91. Letter from Gerald Leitner, Secretary-General, International Federation of Library Associations and Institutions (2016).

92. Keller, *supra* note 73, p. 326.

93. Art. 17 of GDPR.

94. *Ibid*.

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

First, the personal data are no longer necessary for the purposes for which they were collected or otherwise processed.[95] Second, the data subject withdraws their consent to processing and no other ground can justify the processing.[96] Third, the data subject objects to the processing and no overriding legitimate grounds can justify the processing.[97] Fourth, the personal data have been unlawfully processed or must be erased for other reasons.[98] However, the right to be forgotten should not be applied when the processing of personal data is necessary for exercising the right to the freedom of speech, for reasons of public interest, scientific or historical research, or statistical purposes in according to law.[99]

Besides the right to be forgotten, a data subject also has the right to restrict the processing of his or her personal data.[100] The right to restrict processing differs from the right to be forgotten in that the former does not require the data's erasure—rather, it merely restricts their processing.[101] The right to restrict processing can be exercised in four circumstances.[102] First, a data subject can restrict a controller to process his or her personal data when the data subject contests the accuracy of the data and the controller requires time to verify the accuracy.[103] Second, the processing is unlawful but the data subject does not request erasure, but requests the restriction of their use instead.[104] Third, the data subject requires his or her personal data to establish, exercise, or defend legal claims, although the data controller does not need the personal data for the purpose of processing.[105] Fourth, the data subject contests the legitimate process of his or her personal data and this claim is pending verification.[106]

According to the GDPR, an Internet intermediary should follow a notice-and-take-down procedure to address requests brought by a data subject. An Internet intermediary may first restrict the processing of the data (e.g. making it no longer publicly available) after a data subject requests (the requester) the Internet intermediary to remove his or her personal data produced by a third party.[107] The data controller should review the request according to whether the processing of the personal data is necessary for exercising the right to the freedom of speech, for reasons of public interest, scientific or historical research, or statistical purposes in accordance with the law.[108] Generally, the intermediary should complete the review within one month.[109] Then, the intermediary is to inform the requester of the outcome and communicate the removal request to other controllers processing the same data.[110] For

95. *Ibid*., Art. 17.1(a).
96. *Ibid*., Arts 6, 9, 17.1(b).
97. *Ibid*., Arts 17.1(c), 21.
98. *Ibid*., Arts 17.1(d)–(f), 21.
99. *Ibid*., Art. 17.3.
100. *Ibid*.
101. *Ibid*.
102. *Ibid*.
103. *Ibid*., Art. 18.1(a).
104. *Ibid*., Art. 18.1(b).
105. *Ibid*., Art. 18.1(c).
106. *Ibid*., Art. 18.1(d).
107. *Ibid*.
108. *Ibid*., Art. 17.3.
109. Keller, *supra* note 73, p. 341. It is unclear when the statute of limitations should start to run.
110. Arts 17, 18, 21 of GDPR.

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

valid claims, the intermediary delists or erases the relevant personal data.[111] For invalid claims, it will stop restriction and restore the normal processing of the data.[112] Upon the data subject's request, the intermediary must disclose any contact details of the third party who posts the data subject's data.[113] In most cases, the intermediary has no obligation to inform the third party that the contents were delisted or erased.[114]

Notably, Recital 21 of the GDPR provides that it "is without prejudice to the application of [the E-commerce Directive] in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive."[115] Consequently, the GDPR does not replace the intermediary liability rules of the E-commerce Directive.

In terms of intermediary liability for contents produced by a third party, there are three main differences between the E-commerce Directive and the GDPR. First, the E-commerce Directive imposes liabilities by dividing intermediaries into "mere conduit," "catching," and "hosting." Regarding "hosting," the E-commerce Directive further subdivides this category into scenarios where there exists knowledge of the illegal contents and those without. In contrast, the GDPR divides intermediaries into data controllers and processors. The notice-and-take-down procedure under the GDPR is for data controllers. Second, the GDPR notice-and-take-down procedure requires an intermediary to restrict the processing of relevant data even before the data subject's request has been verified. The E-commerce Directive has no such requirement. Third, unlike the E-commerce Directive, the GDPR requires an intermediary to disclose the identity of the third party who posts the information upon a data subject's request.[116] In conclusion, compared with the E-commerce Directive, the GDPR imposes a higher liability on intermediaries for contents produced by third parties.

The question is whether the E-commerce Directive or GDPR should be applied to an Internet intermediary. If the contents produced by a third party infringes upon other parties' intellectual-property rights or is related to hate speech, the E-commerce Directive should be applied. A difficult case arises where a third party illegally posts personal information of a data subject online: should the E-commerce Directive or GDPR apply? Alternatively, should they be applied jointly? Further, suppose that the data subject requests Google, for instance, to delist the URL linking to the information from its search result: should Google follow the E-commerce Directive or GDPR? According to Corte di Cassazione in Italy, the E-commerce Directive applies to Google before it is notified of the illegal contents produced by a third party,[117] as Google is not a data controller before it is informed of the illegal contents.[118] In contrast, *Google Spain* rules that Google is always a data controller and thus should be subject to data-protection law.[119] Also consider the practical implications of the prohibitive penalty under the GDPR, whereby Google will be more incentivized to

111. *Ibid*.

112. *Ibid*.

113. *Ibid*., Arts 14(2)(f), 15(1)(g).

114. Art. 29 Data Prot. Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain" C-131/12 (2014), 3.

115. Recital 21 of GDPR.

116. Arts 14(2)(f), 15(1)(g) of GDPR.

117. Corte di Cassazione, Cass. sez. tre Penale, 3 febbraio 2014, n. 5107/14 (It.).

118. *Google Spain SL*, 2014 E.C.R. 317, ¶ 7.2.

119. *Ibid*., ¶ 3.

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

follow the GDPR rather than the E-commerce Directive.[120] Due to the long-arm jurisdiction created by the GDPR, courts may be prone to applying the GDPR as well. Hence, it remains to be seen how the courts in the EU will reconcile the E-commerce Directive and GDPR in terms of intermediary liability.

5. CHINA: INTERNET UN-IMMUNITY?

As in the US and the EU, in China, content providers are responsible for contents they produced online or offline.[121] As they are not content providers, Internet intermediaries can enjoy civil immunity—though they are subject to the Chinese version of the notice-and-take-down mechanism. However, the feature of Chinese law for Internet intermediaries is Internet un-immunity. Specifically, this stems from how China does not grant the same broad civil immunity to intermediaries for contents created by a third party as the US. In the EU, mere conduit intermediaries can enjoy civil immunity without being subject to the notice-and-take-down mechanism. In contrast, the Chinese version of the notice-and-take-down mechanism applies to all intermediaries, including mere conduit intermediaries. Further, even after an intermediary properly follows the notice-and-take-down mechanism after being notified, it may be still subject to civil liability in China.

The main Chinese laws regulating Internet intermediaries' liabilities are Chinese Tort Law,[122] Provisions of the Supreme People's Court on Certain Issues Concerning the Application of Law in the Hearing of Cases of Civil Disputes over the Use of Information Networks to Infringe upon Personal Rights and Interests (hereinafter "Provisions of SPC on Information Networks Infringement"),[123] Chinese E-commerce Law,[124] and Chinese Consumer Law.[125]

According to Chinese Tort Law, an Internet user who infringes upon the civil right or interest of another person through the network services provided by an intermediary should assume the tort liability.[126] Chinese Tort Law should be read together with the Provisions of SPC on Information Networks Infringement and Chinese E-commerce Law. In particular, the former concerns online personal right infringement and the latter provides detailed regulations for goods and products sold online.

120. Art. 83(5) of GDPR.

121. Supreme People's Court Judicial Interpretation on Several Issues related to Trial of Defamation Cases, Fashi [1998] No. 26.

122. Chinese Tort Law, promulgated by the Standing Committee of China National People's Congress on 26 December 2009 and effective on 1 July 2010, Order No. 21 of the President of the People's Republic of China.

123. Provisions of the Supreme People's Court on Certain Issues Concerning the Application of Law in the Hearing of Cases of Civil Disputes over the Use of Information Networks to Infringe upon Personal Rights and Interests, promulgated on 21 August 2014 and effective on 10 October 2014.

124. Chinese E-commerce Law, promulgated by the Standing Committee of the National People's Congress on 31 August 2018 and effective on 1 January 2019, Order No. 7 of the President of the People's Republic of China.

125. Chinese Consumer Law, promulgated by the Standing Committee of the National People's Congress on 31 October 1993 and most recently amended on 25 October 2013.

126. Article 37 of Chinese Tort Law also provides that, where a network service provider knows that a network user is infringing upon a civil right or interest of another person through its network services and fails to take necessary measures, it shall be jointly and severally liable with the network user. This is like the first paragraph of Art. 38 of E-commerce Law.

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

5.1 Online Personal Right Infringement

Online infringement of personal rights and interests refers to the infringement of the rights to names/titles, reputation, honour, portraits, and privacy. Article 36 of the Chinese Tort Law creates a civil immunity for the intermediary if it takes necessary measures such as deleting, blocking, or disconnecting the infringing material when receiving notice from the infringed party.[127] The intermediary should be jointly and severally liable with the Internet user if the intermediary has the relevant knowledge that the Internet user is infringing upon a civil right or interest of another person through its network services and fails to take necessary measures.[128] Different from the Chinese E-commerce Law, the Provisions of SPC on Information Networks Infringement provides a notice-and-take-down mechanism as a safe harbour to protect intermediaries from online personal right infringement claims.[129]

According to the Provisions of SPC on Information Networks Infringement, a notice is valid as long as it contains (1) the name and contact details of the notifying party, (2) the URL against which necessary measures are required to be taken or relevant information sufficient to accurately locate the infringing contents, and (3) reasons for deleting the relevant information.[130] Should the intermediary fail to take the necessary measures in a timely manner after being notified, it shall be jointly and severally liable for any additional harm with the network user.[131] The courts will consider whether an intermediary has responded promptly by considering factors such as the nature of its service, the form and accuracy of the valid notice, the types of rights and interests infringed upon by the information, and the extent of the infringement.[132]

Article 9 of the Provisions of SPC on Information Networks Infringement provides that a court should consider the following factors in determining whether the intermediary "has the relevant knowledge": (1) whether the network service provider manually or automatically processes the infringing network information by recommendation, ranking, selection, editing, sorting, revision, or other means; (2) the information management capabilities that the network service provider shall possess, the nature of and ways in which the services are provided, and the possibility thereof for leading to infringement; (3) the types of personal rights and interests infringed upon by the relevant piece of network information, and the degree of obviousness of such infringement; (4) the degree of social impact of the relevant piece of network information, or the volume of website traffic thereof within a certain period of time; (5) whether it is technically possible for the network service provider to adopt measures to prevent infringement, and whether the network service provider has taken reasonable measures accordingly; (6) whether the network service provider has taken corresponding reasonable measures against the repeated infringing acts committed by the

127. Art. 36.1 of Chinese Tort Law.

128. *Ibid*., Art. 36.3.

129. The Chinese E-commerce Law creates a notice-and-take-down mechanism for online intellectual-property infringement, which does not apply to non-intellectual-property infringement. Arts 41–45 of Chinese E-commerce Law.

130. Art. 5 of Provisions of SPC on Information Networks Infringement. Provisions of SPC on Information Networks Infringement specifies the formalities of the notice-and-take-down mechanism under Art. 36 of Chinese Tort Law. The infringed party should notify the intermediary in writing or according to the intermediary's requirement.

131. Art. 36.2 of Chinese Tort Law.

132. Art. 6 of Provisions of SPC on Information Networks Infringement.

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

same network user or the same piece of infringing information; and (7) other relevant factors.[133]

In the EU, the intermediary providing "mere conduit" services is generally immune and has no obligation to follow the notice-and-take-down mechanism. However, the Chinese Tort Law and Provisions of SPC on Information Networks Infringement apply the notice-and-take-down mechanism to all intermediaries.

An example is *Cui Hailiang v. Aiming*.[134] In 2010, Mr Song published a libel posting in relation to Mr Cui on an illegal website. Mr Cui requested that Mr Song delete this posting, but the latter asked for a fee. Mr Cui rejected this, instead filing a police complaint. Mr Song was subsequently imprisoned. However, this libel posting remained online and was republished by Dongjing and seven other websites that used the domain-name-registration service provided by Aiming. Whilst Mr Cui requested Aiming to take necessary measures to stop the spread of this libel post, Aiming did not respond to Mr Cui's notice. Consequently, Mr Cui brought a case against Aiming for online defamation pursuant to Article 36 of the Chinese Tort Law. Here, Aiming argued that the libel posting was published by third-party websites that used its domain-registration service—and thus Aiming has no right to manage and review the postings on these websites; nor did it have an obligation to remove this posting. Article 36 of the Chinese Tort Law does not define the meaning of "network service provider." The court held that domain-name registrars should be considered as a network service provider under Article 36, for two reasons. First, if the domain names of the seven websites that published the posting are not registered with Aiming, these websites cannot be accessed. Second, Aiming may have implemented necessary measures in order to mitigate the harm to Mr Cui, such as suspending its service to the seven websites. Therefore, considering a domain-name registrar as a network service provider can help the infringed party to promptly and effectively safeguard his or her legal right—indeed, such is the underlying policy of Article 36 of the Tort Law. Despite the fact that the libel posting was published by Dongjing and seven websites that were not Aiming, the court held that Aiming was liable to pay damages for its failure to take any action to remove the libel post.

Cui Hailiang v. Aiming was the first online-defamation case in China brought against a domain-name registrar for a posting published by a third party. Notably, from the facts of the case, it is unclear whether Aiming is the sole provider of the conduit service. In *A Network Technology Co., Ltd of Hangzhou v. A Network Technology Co., Ltd of Changsha and Shenzhen Tencent Computer System Col, Ltd*, the Zhangzhou Internet Court held that WeChat's mini-programme service provider can enjoy civil immunity without being subject to the notice-and-take-down mechanism,[135] as the mini-programme service provider only provides auto-access, auto-transmission, and other basic network services. The Internet Court held that the term "network service provider"—as mentioned in the notice-and-take-down mechanism in Article 36 of the Chinese Tort Law—refers to the network service provider that provides information storage space or search, link, or other services. Essentially, like the EU E-commerce Directive, *A Network Technology Co., Ltd of*

133. Art. 9 of Provisions of SPC on Information Networks Infringement.

134. *Cui Hialiang v. Hanzhou Aiming Network Co Ltd and Hanzhou Dayi Shangwu Network Co Ltd*, Henan Xinxiang Intermediate People's Court (2013) Xin Zhong Min Shi Zong Zi No. 178.

135. Chinalawinfo.com (2019).

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

Hangzhou demonstrates that mere conduit intermediaries should be immune from contents produced by third parties and should not be subject to the notice-and-take-down mechanism. However, as an intellectual-property infringement case, *A Network Technology Co., Ltd of Hangzhou* is unclear as to whether its interpretation of Article 36 of Chinese Tort Law holds true for non-intellectual-property cases. Moreover, China is not a case-law country; thus, this case does not create a precedent. Therefore, whether the notice-and-take-down mechanism should be applied to mere conduit intermediaries in China has yet to be clarified.

5.2 Torts Related to Goods and Products Sold Online

Article 44.2 of the Chinese Consumer Law provides that, if an e-commerce platform provider (i.e. intermediary), first, knows, or should have known, that a dealer who sells a product or service on its platform is infringing upon the consumer's right and interest, and, second, does not take any necessary measures, the platform provider shall be jointly and severally liable to the consumer with the dealer. Article 44.2 of the Chinese Consumer Law provides a general requirement and Article 38.1 of the E-commerce Law is *lex specialis*. It particularizes a specific circumstance of violation: where an e-commerce platform provider both knows or ought to know that the products or services provided by a dealer over its platform fail to meet the requirements *for the protection of personal and property safety*, and fails to take the necessary measures, the platform provider and the operator shall bear joint and several liability for the aforesaid violations.[136] Namely, as long as an e-commerce platform provider takes necessary measures, it will be immune from the liability relating to the products or services provided by the dealer over its platform. Article 36 of the Chinese Tort Law provides that, where a network user commits a tort through the network services, the victim of the tort shall be entitled to notify the network service provider to take necessary measures such as deletion, block, or disconnection.[137] Therefore, the "necessary measures" under Article 38.1 of the Chinese E-commerce Law and Article 44.2 essentially denotes the notice-and-take-down mechanism. However, neither the Chinese Tort Law, Chinese E-commerce Law, or the Chinese Consumer Law provides details of the notice-and-take-down mechanism. Courts may refer to the Provisions of SPC on Information Networks Infringement that provides details of the notice-and-take-down mechanism.

Suppose a platform provider properly follows the notice-and-take-down mechanism after receiving a consumer's notice: will the platform provider be immune from the liability relating to the defective products or service sold by the dealer? The answer is in the negative. The reason for this resides in how Article 38.1 should be read together with Article 44.1 of the Chinese Consumer Law. Precisely, the latter provides that, if a platform provider cannot provide the true name, address, or contact information of a dealer selling products or services on its platform, the consumer can request the platform to cover the damages that the consumer suffered from the defective product or service.[138] Therefore, compared with the laws of the US and the EU, the Internet immunity in China is much more restricted.

In the US, however, constructive knowledge without affirmative action cannot deprive an e-commerce platform provider of immunity unless they have actual knowledge of the illegal

136. Art. 38.1 of Chinese E-commerce Law.
137. Art. 36 of Chinese Tort Law.
138. Art. 44.1 of Chinese Consumer Law.

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

online materials produced by third parties. For example, *Randall Stoner v. eBay Inc., et al.* concerns "bootlegs," which are unauthorized recordings of a live musical performance.[139] eBay, through their online auction platform, facilitates sales by services such as notices, payment, insurance, and escrow. The plaintiff argued that eBay should be responsible for its own participation in selling bootlegs. The plaintiff further asserted that eBay failed to monitor the products auctioned on its service platform because "[t]he very description of some [the] recordings (e.g. 'bootleg' tapes) identifies some as contraband."[140] The California Superior Court of San Francisco rejected both claims, holding that eBay is an interactive service provider (i.e. intermediary) and was therefore protected by the immunity clause under CDA § 230. This is due to the fact that the information concerning bootlegs came from third-party users. Even if eBay were to identify these products as contraband, the court held that Congress would have intended to remove any legal obligations of interactive computer service providers that may have attempted to identify or monitor the sale of illegal products, as "the threat of liability for failing to monitor effectively would … deter companies such as eBay from making their service available as widely and as freely as possible."[141] Moreover, removing any legal obligation to monitor aims encourages self-regulation. Therefore, the plaintiff must prove "actual, rather than constructive knowledge of illegal sales, and some affirmative action by the computer service, beyond making its facilities available in normal manner, designed to accomplish the illegal sales."[142] In contrast to the US CDA § 230, paragraph 1 of Article 38 of the Chinese E-commerce Law allows the evidence of constructive knowledge to deprive an e-commerce platform provider of immunity. This is another reason that intermediaries in China enjoy far less civil immunity.

More importantly, dissimilar to Article 38.1, Article 38.2 of the Chinese E-commerce Law imposes a general obligation on the e-commerce platform provider to review the qualifications or certificates of the dealers who sell goods or services related to the consumer's life and health through the platform managed by the e-commerce platform provider.[143] This general obligation will not be exempted by the notice-and-take-down mechanism. The e-commerce platform provider will lose its immunity if it fails to review the qualifications or certificates of operators or fails to fulfil the safety guarantee obligations to consumers, thereby causing harm to them. Notably, Article 38.2 of the Chinese E-commerce Law only addresses goods or services related to the consumer's life and health, while Article 38.1 applies to all other goods or services sold online. Besides the different scopes of application, consumers may find it more difficult to satisfy their burden of proof under Article 38.2 than that under Article 38.1. To make a claim under Article 38.1, consumers must prove that the e-commerce platform providers had actual or constructive knowledge of the defective products or services provided by a third party and that the e-commerce platform providers failed to take action against them. Proving that the e-commerce platform provider had actual or constructive knowledge may be accomplished by providing the notice that was sent by

139. In *Randall Stoner v. Ebay Inc., et al.* 2000 WL 1705637, Civ. No. 305666 (Sup. Ct. Ca., November 7, 2000). Plaintiff's claim is not based on the federal Copyright Act; instead, the plaintiff claims that these sales violated California Business and Professions Code.

140. *Ibid.*

141. *Ibid.*

142. *Ibid.*

143. Para. 2 of Art. 38 of Chinese E-commerce Law.

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

the consumer informing the platform provider of the violation. However, it is not an easy task for a consumer to prove that an e-commerce platform provider has probably reviewed the dealer's qualifications or certificates or that the dealer has fulfilled its safety guarantee—especially when the review process and safety guarantee are embodied by internal documents adopted by the platform provider. Even if these documents are publicized online openly, it is still difficult for the consumers to prove whether they have been properly implemented by the platform provider.

On the other hand, the intermediary's liability under Article 38.2 of the E-commerce Law needs clarification in four aspects.

First, the scope of "goods or services related to [a] consumer's life and health" is not defined. For instance, medicine can be considered as a product related to a consumer's life and health. However, whether a product such as a car or car tyre falls into this category remains unclear. The ambiguity of "goods or services related to consumer's life and health" brings uncertainty to the obligations of e-commerce platform service providers.

Second, no clear guidelines are provided for an e-commerce platform provider to review the qualifications or certificates of dealers in different industries who sell products and services on the platform. Article 27 of the E-commerce Law provides that, where a dealer applies to an e-commerce platform operator to use the platform to sell products or provide services, the latter shall ask the former to submit authentic information concerning the dealer's identity, address, contact information, and administrative licence; verify the information submitted; and periodically verify and update the files and related information. Article 27 applies to all dealers conducting online sales using the platform provided by e-commerce platform providers. It is unclear whether e-commerce platform providers should extend beyond the requirements listed in Article 27 and request more information about the qualifications and certificates for dealers selling goods and services related to consumers' life and health. This seems to be justified, as Article 38.2 aims to provide enhanced protection to consumers who buy goods or services related to their lives and health. Hence, e-commerce platform providers ought to bear a higher burden of proof and request more documents than those listed in Article 27. Although this argument seems valid in a theoretical sense, it is in reality difficult to implement. For example, the qualifications and certificates for dealers in the pharmaceutical industry are significantly different from those in the automobile industry. It is, therefore, difficult to determine what sort of detailed information an e-commerce platform provider should request from a dealer in order to satisfy its review obligations under Article 38.2. Arguably, if an e-commerce platform provider has exercised due care in reviewing and verifying documents under Article 27, the provider should be considered as having satisfied its review obligation under Article 38.2. Article 38.2 provides enhanced protection for consumers by removing their burden of proof in demonstrating whether the platform provider knew or should have known that the product or service was defective. In other words, protection is afforded where an e-commerce platform provider fails to duly review the qualifications and certificates of dealers under Article 27 and a consumer suffers harm due to a defective product or service. The consumer can then request the e-commerce platform provider to bear the relevant liabilities according to law.

The third issue in relation to Article 38.2 is the ambiguity of the "safety guarantee obligations for consumers." Does the "safety guarantee" refer solely to a duty implied by law on the platform provider to adopt safety protection measures? One argument is that the duty is

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

the same as the duty imposed by Article 37 of the Chinese Tort Law on all persons responsible for managing hotels, shopping malls, banks, and other public places, as well as all persons organizing mass activities. If this argument is true, Article 38.2 of the Chinese E-commerce Law would have explicitly indicated that the platform provider should assume complementary liability as Article 37 of the Chinese Tort Law does. Complementary liability means that the third party should bear the liability first-hand and managers or organizers will be liable only when the third party fails to pay damages in cases such as bankruptcy. Article 38.2 of the Chinese E-commerce Law does not mention complementary liability. "Safety guarantee" under Article 38.2 of the Chinese E-commerce Law should go beyond the duty imposed by Article 37 of the Chinese Tort Law. It may refer to explicit guarantees provided by an e-commerce platform provider, such as a statement that the quality of all products sold on its platform is guaranteed. The courts should be allowed to hold the e-commerce platform provider's implied guarantees by construing the user's agreement or online advertisements.

Lastly, unlike Article 38.1 of the E-commerce Law that imposes joint and several liability on the e-commerce platform providers, Article 38.2 does not specify the liability of an e-commerce platform provider.[144] The legislative history of Article 38 demonstrates tensions between protecting online consumers and promoting the growth of e-commerce platforms. E-commerce platform providers have strongly advocated that they should be treated as the managers of public venues such as brick-and-mortar hotels, shopping centres, banks, stations, or entertainment places, or organizers of mass activities in real life under Article 37 of the Chinese Tort Law. Accordingly, if the harm to another person is caused by a third party, the third party should assume tort liability while the managers or organizers, should they fail to fulfil the duty or provide safety guarantee, should assume the corresponding complementary liability.[145] Applying Article 37 of the Chinese Tort Law to e-commerce platform providers was severely criticized by the general public upon the release of the E-commerce Bill in early 2018.[146] Opponents argue that e-commerce platform providers should be distinct from managers of brick-and-mortar hotels and shopping centres, and should not enjoy the protection granted by Article 37 of the Chinese Tort Law. This is partly due to the boom in Chinese e-commerce, resulting in a drastic increase in consumer complaints related to defective products or services sold online and an increasing difficulty in locating online shop operators to hold them responsible. This issue is exacerbated when Chinese e-commerce platform providers offer platforms to foreign shop operators for them to sell their products or services to Chinese consumers. Consumers find it challenging to hold foreign shop operators liable for defective products and misrepresentation. Further, criticisms also stemmed from the fact that Chinese Internet sales platforms are highly monopolized by only a few e-commerce platform providers, such as Alibaba, JD, Ctrip, etc. The inequality between e-commerce platform providers and consumers requires a policy choice against the extension of Article 37 to e-commerce platform providers. Though these

144. Para. 2, Art. 38 of Chinese E-commerce Law provides that the e-commerce platform operator shall be held liable correspondingly according to law.

145. Art. 37 of Chinese Tort Law.

146. Xinhuanet.com (2018).

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

criticisms have gained support from a few members in the Chinese NPC Standing Committee,[147] it seems that consumer protections remain insufficient to drive Chinese legislators to pass a clear policy choice favourable to consumers. Although consumer protection may gain public popularity in China, Chinese legislators will not make an explicit policy choice favourable to consumers without the proper constitutional support. Moreover, the e-commerce platform providers strongly lobbied against joint and several liability with online shop operators in cases where they failed to review the latter's qualification or fulfil the safety guarantee obligations for consumers. Although the Chinese government has an interest in facilitating the development of the domestic e-commerce industry, the government, however, is also concerned that it is imposing too many obligations on e-commerce platform providers that may ultimately increase the online transaction costs that consumers would have to pay. Consequently, Article 38.2 of the E-commerce Law does not clearly specify an e-commerce platform provider's liability. Instead, it provides that the issue of liability should be determined according to the relevant laws.

6. CONCLUSION

This paper argues that the US applies broad civil immunity to intermediaries and exempts them from civil liability arising from contents produced by third parties. Both the EU and China restrict civil immunity to intermediaries that meet the notice-and-take-down requirement. Chinese law is different from the US and the EU law in two important respects.

First, contemporary Chinese law imposes either higher liabilities (as compared with the US) on Internet intermediaries or unclear procedures to be immune (as compared with the EU). This is because, unlike US law, Chinese law does not grant absolute immunity to intermediaries. Nor does China divide intermediaries into categories of "mere conduit," "caching," and "hosting"—as per the EU—and applies the notice-and-take-down mechanism differently. Instead, intermediaries in China may be subject to civil liability even if they properly follow the notice-and-take-down mechanism that the Chinese Consumer Law provides. Moreover, it is unclear whether the "mere conduit" intermediaries can enjoy civil immunity without being subject to the notice-and-take-down mechanism in China.

Second, unlike the US and the EU—both of which have made explicit policy a priority regarding liabilities that Internet intermediaries should bear—Chinese policy choices are unsettled. The US law for intermediaries' liability focuses on protecting the free flow of information under the First and Fourteenth Amendments of the US Constitution. In contrast, the EU emphasizes the protection of personal information as a fundamental human right. Yet, China has not made a clear policy choice. Consumer protection has boomed in public popularity and increasingly attracted the attentions of the legislature and judiciary in China. However, it is doubtable that the protection of consumers can provide a prevailing policy support for Chinese law in the same way as freedom of speech and the protection of personal information do under the laws of the US and the EU. This is because protecting consumers is a vague concept. It is fundamentally different from the freedom of speech and the protection of personal information that have direct constitutional supports in the US and the EU, respectively. Indeed, the legislative history of the Chinese E-commerce Law as discussed

147. *Ibid*.

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

above also demonstrates that protecting consumers may not outweigh other competing considerations such as protecting intermediaries and developing e-commerce.

REFERENCES

Ballard Spahr LLP (2018) "New Trade Agreement Extends CDA Section 230 Immunity Abroad," https://www.ballardspahr.com/alertspublications/legalalerts/2018–10–04-new-trade-agreement-extends-cda-section-230-immunity-abroad (accessed 31 October 2019).

Bluebond, Andrew (2014) "When the Customer Is Wrong: Defamation, Interactive Websites, and Immunity." 33 *Review of Litigation* 679–710.

Cecil, Amanda L. (2014) "Taking Back the Internet: Imposing Civil Liability on Interactive Computer Services in an Attempt to Provide an Adequate Remedy to Victims of Nonconsensual Pornography Note." 71 *Washington and Lee Law Review* 2513–66.

Chinalawinfo.com (2019) "No. 5 of the Ten Influential Cases on the Occasion of the Second Anniversary of the Establishment of the Hangzhou Internet Court (Part Two)," www.chinalawinfo.com (accessed 31 October 2019).

Congress.gov (2017–18) "H.R.1865—Allow States and Victims to Fight Online Sex Trafficking Act of 2017," https://www.congress.gov/bill/115th-congress/house-bill/1865 (accessed 31 October 2019).

Electronic Frontier Foundation.org (2019) "CDA 230: Key Legal Cases," https://www.eff.org/issues/cda230/legal (accessed 31 October 2019).

eMarketer.com (2019) "Global Ecommerce 2019," https://www.emarketer.com/content/global-ecommerce-2019 (accessed 7 October 2019).

Goldman, Eric (2017) "The Ten Most Important Section 230 Rulings." 20 *Tulane Journal of Technology and Intellectual Property* 1–10.

Goldman, Eric (2019) "Why Section 230 Is Better Than the First Amendment." *Notre Dame Law Review Online* (Forthcoming).

Jackman, Tom (2018) "Trump Signs 'FOSTA' Bill Targeting Online Sex Trafficking, Enables States and Victims to Pursue Websites," *The Washington Post*, 12 April.

Keller, Daphne (2018) "The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation." 33 *Berkeley Journal of International Law* 287–369.

Khanna, Derek (2013) "The Law That Gave Us the Modern Internet and the Campaign To Kill It," *The Atlantic*, 12 September.

Kozak, Nadine Irène (2018) "Fighting for the Internet: Online Blackout Protests and Internet Legislation in the United States, 1996–2018." 21 *M/C Journal*, http://journal.media-culture.org.au/index.php/mcjournal/rt/printerFriendly/1415/0 (accessed 31 October 2019).

Kuner, Christopher (2015) "The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges," in B. Hess and C. M. Mariottini, eds., *Protecting Privacy in Private International and Procedural Law and by Data Protection*, Baden-Baden: Nomos, 19–55.

Letter from Gerald Leitner, Secretary-General, International Federation of Library Associations and Institutions (2016) "Application of Right to be Forgotten Rulings: The Library Viewpoint," https://www.ifla.org/files/assets/faife/statements/161024_ifla_on_rtbf_case_in_france.pdf (accessed 31 October 2019).

Letter from Josh King, CEO, Avvo, to Honorable Tani Cantil-Sakauye, Chief Justice, Supreme Court of the State of California (2016), http://digitalcommons.law.scu.edu/cgilviewcontent.cgi?filename=4&article=2266&context-historical&type=additional (accessed 31 October 2019).

Media Legal Defence Initiative.org (2015) "Freedom of Expression, Media Law and Defamation," https://www.mediadefence.org/sites/default/files/resources/files/MLDI.IPI%20defamation%20manual.English.pdf (accessed 31 October 2019).

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press

OECD.org (2010) "The Economic and Social Role of Internet Intermediaries," https://www.oecd.org/internet/ieconomy/44949023.pdf (accessed 31 October 2019).

Office of the United States Trade Representative.gov (2018) "United States-Mexico-Canada Agreement," /trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement (accessed 10 September 2019).

Pappalardo, Kylie, & Nicolas Suzor (2018) "The Liability of Australian Online Intermediaries." 40 *Sydney Law Review* 469–98.

Peguera, Miquel (2016) "The Shaky Ground of the Right to Be Delisted." 18 *Vanderbilt Journal of Entertainment & Technology Law* 507–61.

Reason.com (2018) "Facebook Supported 'Sex Trafficking' Law FOSTA to Cozy Up to Republican Critics: Reason Roundup," https://reason.com/2018/11/15/how-facebook-sold-out-sex-workers/ (accessed 15 November 2018).

Stewart, Daxton R. (2013) "When Retweets Attack: Are Twitter Users Liable for Republishing the Defamatory Tweets of Others?" 90 *Journalism & Mass Communication Quarterly* 233–47.

Transparencyreport.google.com (2019) "Requests to Delist Content under European Privacy Law," https://transparencyreport.google.com/eu-privacy/overview?hl=en (accessed 31 October 2019).

World Trade Organization (2019) "Joint Statement on Electronic Commerce," WT/L/1056, Geneva.

Xinhuanet.com (2018) "Why Did E-commerce Law Experience 'Four Read'?," –http://www.xinhuanet.com/politics/2018–09/12/c_1123415183.htm. (accessed 31 October 2019).

Zara, Christopher (2017) "The Most Important Law in Tech Has a Problem," *WIRED*, 1 March.

https://doi.org/10.1017/als.2019.27 Published online by Cambridge University Press