Research Office
Legislative Council Secretariat

Information Note

Internet freedom and regulation in selected places

IN17/19-20

1. Introduction

1.1 In the digital environment of today, the majority of online communications are conducted over the networks or platforms controlled by online service providers ("OSPs"[1]).[2] While OSPs enable individuals to engage in new forms of expression and transaction, Internet users in turn contribute large amounts of content on these platforms. Depending on the context, OSPs may merely play a passive role in hosting user-generated content, or they may exert more direct forms of control[3]. This has engendered discussions on (a) whether OSPs would be held liable for illicit content such as copyright infringement and hate speech posted by their users; and (b) whether the freedom of Internet users ("Internet freedom") would be affected by the measures of content moderation adopted by OSPs. Internet freedom – including the freedom of expression, access to information and right to privacy – are considered as extensions of the equal and inalienable rights laid out in the Universal Declaration of Human Rights ("UDHR") and the International Covenant on Civil and Political Rights ("ICCPR").[4]

1.2 Apart from online content, some Internet users have also provided their personal information to online platforms. Like other business entities, OSPs are generally required to observe the relevant laws in collecting, using and disclosing personal data. Yet, Internet users may be exposed to additional privacy risks particularly when OSPs (a) collect and process sensitive personal data such as political opinions or biometrics; (b) use automation to profile, evaluate or make decisions affecting them[5]; or (c) adopt cross-border

---

1 OSPs broadly refer to online intermediaries such as Google, Twitter and Facebook which give access to, host, transmit and index content and products originated by third parties on the Internet. See Organisation for Economic Co-operation and Development (2010).

2 See Stanford Law School (2020).

3 For instance, OSPs may use their own algorithms to determine the order in which some content appear before others, or they may use upload filters to prohibit some types of content at the point of upload.

4 According to a resolution passed by the United Nations in 2016, "the same rights that people have offline must also be protected online". See United Nations (2016).

5 Examples of automated decision-making include online credit applications and e-recruitment.

data transfers as part of the service provided[6]. These have given rise to discussions on whether data rights should be enhanced to safeguard data subjects against the privacy risks attendant to data processing.

1.3 The United States ("US") and the European Union ("EU") are home to sizable Internet markets in terms of the number of users[7] and scale of electronic commerce[8]. Regarding the freedoms of expression and information on the Internet, the US passed the Communications Decency Act in 1996 to define the intermediary liability of OSPs. In general, OSPs are not liable for their voluntary decisions to host or delete user-generated content, nor are they required to monitor their platforms for illicit activities. Yet, copyright infringement is an exception as OSPs are required to take down such content upon receiving a valid notice from copyright holders. The US regime has been credited for respecting Internet freedom and spurring the growth of major OSPs like Google, Facebook and Twitter.[9] As to personal data privacy protection, there is no overarching legislation in the US governing privacy rights of Internet users. Nevertheless, there are separate federal laws to protect consumers from unfair or deceptive data practices.

1.4 In comparison, the EU safeguards the freedoms of expression and information as well as the right to privacy with equal respect. It introduced the e-Commerce Directive in 2000 specifying that there is no general obligation on OSPs to monitor the information on their platforms. Nevertheless, OSPs are still required to observe EU laws and voluntary codes of practices to expeditiously remove all illegal online content upon receiving a valid notice. In recent years, OSPs have been subject to additional restrictions imposed on specific types of content such as copyright infringements, hate speech and disinformation[10]. As to personal data protection, the General Data Protection Regulation codifies the various rights enjoyed by data subjects and regulates cross-border data transfer. It also adopts a risk-based approach in limiting the use of sensitive personal data and the scope of automated decision-making.

---

6 For instance, cross-border data transfers may occur when Internet users upload their personal data on cloud storage.

7 In 2017, there were around 351 million and 284 million Internet users in the EU and the US respectively. See The World Bank (2019) and Our World in Data (2019).

8 For instance, the US and the EU Member States of Germany and France were ranked among the global top 10 countries in terms of the amount of e-commerce sales in 2019. See eshopworld (2018) and Oberlo (2019).

9 See Electronic Frontier Foundation (2020).

10 Disinformation is false or misleading information deliberately and often spread covertly in order to influence public opinion or obscure the truth.

1.5 In Hong Kong, there is generally no restriction to Internet access and online censorship has, until most recently, not been an issue for the territory. The question of OSP liability was first discussed during the deliberation of the Copyright (Amendment) Bill in 2014; whereas the application for an interim injunction against the "promotion, encouragement and incitement of the use or threat of violence via Internet-based platform or medium" in October 2019 has reignited the discussion. The recent government proposals to strengthen the existing legislation for personal data privacy has added to the discussions on whether data subjects are adequately protected from the privacy risks found online.

1.6 At the request of Hon Alvin YEUNG, the Research Office has prepared this information note on Internet freedom in Hong Kong, with special reference to recent regulatory developments in online content regulation and personal data privacy protection. The information note also studies how the US and the EU strike a balance between Internet freedom and online regulation (**Appendix I**), covering the legal basis, regulatory approaches, safeguards and remedies related to the regulation of online speech and content. The personal data privacy protection regimes adopted by them are also studied (**Appendix II**).

2. Internet freedom in Hong Kong

2.1 In Hong Kong, the freedoms of expression, information and privacy are safeguarded by Chapter III of the Basic Law and the Hong Kong Bill of Rights Ordinance ("HKBRO") (Cap. 383). HKBRO is the domestic enactment of ICCPR as applied to Hong Kong.[11] It is binding on the Government and all public authorities, and the rights it affords are generally applicable except in times of public emergencies[12]. HKBRO specifies that the freedom of expression applies regardless of frontiers or media, and that it may only be subject to restrictions which are provided by law and necessary for (a) respect of the rights or reputations of others; or (b) the protection of national security or of public order, public health or morals.[13]

---

[11] China has signed but not yet ratified ICCPR. See United Nations Treaty Collection (2020).

[12] Section 5 of HKBRO specifies that measures may be taken in times of public emergency to derogate from the Bill of Rights to the extent strictly required by the exigencies of the situation. See Hong Kong e-Legislation (2017).

[13] Similar restrictions are found in ICCPR as well as the European Convention on Human Rights.

Regulation of online content and speech

2.2 In Hong Kong, illicit online content such as copyright infringements, speech inciting the use or threat of violence, and other criminal material are subject to regulation and enforcement by the authorities.[14] There is no restriction to Internet access and online censorship has thus far not been an issue for the territory.[15] In recent years, some developments on the legal front have precipitated discussions on the role of OSPs in regulating online speech and content.

Discussions on OSP liability during the Copyright (Amendment) Bill 2014

2.3 Under the existing copyright legislation in Hong Kong, copyright holders have the exclusive rights to copy and distribute their work. Any person who, without the consent of the rights holder, violates these exclusive rights may be liable for **primary infringement**. Furthermore, a person may be liable for **secondary infringement** if he or she knowingly[16] possesses or deals with infringing copies of copyright works. In the digital environment, the intermediary role played by OSPs means that they may not be aware of the infringing activities on their platforms. This has precipitated discussions as to whether OSPs should cooperate with rights holders to tackle copyright infringements on their platforms and, if so, whether the freedom of expression of Internet users would be affected.

---

[14] The Government and other public bodies have submitted requests to information and communication technology companies for disclosure of user data and removal of online content for law enforcement purposes such as the prevention/detection of crime, stoppage of infringing activities, and action against the illegal sales of medicine. See GovHK (2019).

[15] The US Department of State compiles the annual Country Report on Human Rights Practices in China (Includes Hong Kong, Macau, and Tibet). In the section on Hong Kong, the report has consistently stated that the Hong Kong Government did not restrict or disrupt access to the Internet or censor online content. See US Department of State (various years).

[16] The person will only be liable if, at the time he or she committed the act, he or she knew or had reason to believe that he or she was dealing with infringing copies. If such knowledge or guilty state of mind cannot be proved, that person will not be liable for secondary infringement. See CLIC (2018).

2.4 The discussion on the **intermediary liability** of OSPs emerged in June 2014, when the Government introduced the Copyright (Amendment) Bill 2014[17]. Among others, the Bill proposed a set of "safe harbour" provisions so that OSPs are only subject to limited liability for copyright infringements on their platforms. OSPs would be protected by the "safe harbour" as long as they remove any alleged infringing content upon receiving valid notices from copyright holders. However, OSPs were not required to actively monitor their platforms for infringing activities, and content uploaders could submit counter notices to contest the takedown decisions.

2.5 According to the Commerce and Economic Development Bureau[18], the "notice-and-takedown" regime outlined above[19] would incentivize OSPs to cooperate with rights holders to tackle copyright violations. Indeed, rights holders generally supported the "safe harbour" provision because it provided a mechanism to tackle online infringements without resorting to court proceedings.[20] OSPs also expressed support as the "notice-and-takedown" would provide greater clarity as to their liability for user-generated content.

2.6 Notwithstanding this, some Internet users and concern groups still questioned whether the implementation of "notice-and-takedown" might be subject to abuse. While both rights holders and content uploaders were required to submit information in good faith,[21] it was argued that there were no safeguards to prevent OSPs from erring on the side of safety and taking down legal or exempted[22] content. There were also concerns that users had limited recourse to challenge OSPs' takedown decisions. Due to the strong public opposition, the Copyright (Amendment) Bill 2014 lapsed at the end of the term of office of the Fifth Legislative Council in 2016.

---

17 The Bill was introduced in June 2014 to update Hong Kong's copyright regime. A technology neutral right for copyright holders to communicate their works was introduced to keep pace with technological changes such as online streaming.

18 See Commerce and Economic Development Bureau (2014).

19 The proposed "notice-and-takedown" is based on a similar regime in the US.

20 See Motion Picture Association (2014).

21 Submission of false statements by either party may be liable to civil and/or criminal sanctions.

22 Under the proposed Bill, the exempted content would have included fair dealings of copyright material involving parody, quotation, and/or commentary of current events.

Discussions on OSP liability for online content inciting violence

2.7 Following the outbreak of social incident in June 2019, there were views that the Internet had played a role in inciting violence and vandalism on the streets. On 31 October 2019, the High Court handed down an interim injunction[23] against the "promotion, encouragement and incitement of the use or threat of violence via Internet-based platform or medium". The interim injunction also prohibited any person from aiding or authorizing others to commit the above acts.

2.8 The interim injunction gave rise to discussions as to whether OSPs would breach the court order simply because Internet users posted inciting material on their platforms. In order to clarify this, the Internet Society Hong Kong filed an application seeking to discharge or modify the order.[24] Subsequently, the High Court amended its injunction to only restrain those who **willfully** assist others to post inciting material online. In other words, OSPs are not in breach of the injunction even if they enable posts to be made on their platforms, without knowing the facts or contents of such publication. Furthermore, the injunction does not impose a positive duty on OSPs to search for or filter out unlawful content uploaded by others.[25]

Protection of online data privacy

2.9 In Hong Kong, the Personal Data (Privacy) Ordinance ("PDPO") (Cap. 486) protects the personal data privacy of individuals. PDPO is a technology neutral[26] legislation which regulates the collection, use and disclosure of personal data in online and offline situations. It requires data users[27] including OSPs to ensure that personal data is collected on a fully-informed basis, processed in a secure manner, and used only in relation

---

[23] According to the Secretary for Justice, she applied for the interim injunction as guardian of the public interest to take action to restrain public nuisance. The High Court recognized that the order may restrict fundamental rights, but considered the terms of the injunction as a justified and proportionate restriction on speech inciting violence. See Legal Reference System (2019).

[24] Apart from OSP liability, the Internet Society Hong Kong also had concerns that the terms of the injunction were overbroad and might adversely impact the operation of Internet infrastructure, and the freedom of expression of Internet users. The Society comprises members working in the development, operation and use of Internet connected and Internet-based applications, platforms and media. See Internet Society (2019) and Internet Society Hong Kong (2019).

[25] See Legal Reference System (2019).

[26] Technology neutral means the same regulatory principles apply regardless of the technology.

[27] Data user is a person who controls the collection, holding, processing or use of personal data.

to the original purpose of collection.[28] It also grants data subjects[29] the rights to request access to and correction of their own personal data.

2.10 Following a number of large-scale personal data leakage incidents,[30] the Government announced that it is working with the Office of the Privacy Commissioner for Personal Data ("PCPD") to amend PDPO to strengthen personal data protection in Hong Kong. These include (a) requiring mandatory data breach notifications; (b) strengthening the regulation on data processors; and (c) expanding the definition of personal data[31]. Yet, in light of the increased bulk, frequency and innovative ways in which personal data is being processed online, there are discussions as to whether data rights should also be enhanced in the following areas to counter the privacy risks involved:[32]

(a) **processing of sensitive personal data**: some OSPs increasingly collect, use or even profit from their users' sensitive personal data including political opinions and biometrics[33]. Although consent must be obtained before processing any type of personal data, there are views that the use of sensitive personal data should be subject to further conditions. These include granting data subjects the rights to restrict or opt out from the use of their sensitive personal data.[34]

(b) **automated decision-making**: automation is increasingly used to analyse, predict or profile certain personal aspects of Internet users. In cases such as e-recruitment and online credit applications, automation may be used to make significant decisions regarding individuals. Although PDPO is technology neutral, there are views that further restrictions should apply so that data subjects can contest decisions that are made solely by automation; and

---

28 While contravention of these principles is not an offence, the Office of the Privacy Commissioner for Personal Data may conduct investigations and serve enforcement notices requiring data users to remedy or desist from such contravention. Violation of an enforcement notice is an offence.

29 Data subject is the individual who is the subject of the personal data.

30 For example, Cathay Pacific in October 2018 unveiled the leakage of personal data relating to 9.4 million of its passengers. See Office of the Privacy Commissioner for Personal Data (2019).

31 See Constitutional and Mainland Affairs Bureau (2020).

32 See Legislative Council Secretariat (2020) and Human Rights Watch (2020).

33 This includes, for instance, the processing of fingerprints, retina scans and facial images.

34 According to the Government, expanding the definition of personal data from data relating to an "identified" person to data relating to an "identifiable" natural person already enhances the level of protection. See Constitutional and Mainland Affairs Bureau (2020).

(c) **cross-border data transfer**: the use of cloud storage and remote data access has resulted in more frequent transfer of data across jurisdictions. Under Section 33 of PDPO, personal data in Hong Kong should only be transferred to overseas places which are certified by PCPD's "white list" of places with similar data protection laws, or consent has been given by the data subject. Yet, the implementation of Section 33 has been held back due to concerns raised by the business sector.[35]

3. Internet freedom in the United States

3.1 In the US, the freedom of expression is safeguarded by the First Amendment to the US Constitution[36]. A core tenet of the First Amendment is to foster "an uninhibited marketplace of ideas", prizing "more speech" over less or none[37]. In contrast, the right to privacy is not expressly enshrined in the US Constitution.[38] Nevertheless, some provisions such as the Fourth and Fourteenth Amendments have been interpreted to protect personal privacy from government intrusion.[39] A number of federal legislation are also in place to protect the personal data of individuals and consumers.

3.2 The strong tradition of the US in upholding free speech applies to the Internet, where users engage in an array of free speech activities. Nevertheless, the extent of free speech protection for Internet users is by no means absolute, as evidenced by varying degrees of protection afforded to different categories of speech. For instance, the government may enact laws to regulate unprotected speech, such as obscenity, defamation, fraud, and incitement[40]. On the other hand, **hate speech** which merely demeans on the

---

35 The business sector has concerns over the (a) impact on operations, e.g. impact on international trade and online sales; and (b) difficulties in compliance, e.g. lack of resources and legal knowledge. PCPD is currently studying the issues raised and the related compliance matters.

36 The First Amendment protects the right to freedom of expression from government interference. It prohibits the Congress from making any laws that abridge the freedom of speech. See Congressional Research Service (2019b).

37 See Taruschio (2000).

38 This is in part because the US Constitution as it was conceived afforded less weight on the right to privacy. See Congressional Research Service (2019a).

39 The Fourth Amendment protects individuals from unreasonable searches, arbitrary arrest and surveillance, whereas the Fourteenth Amendment provides that individuals shall not be deprived of their liberty without due process of law. See Congressional Research Service (2019a).

40 See Congressional Research Service (2019e).

basis of race, ethnicity or gender remains protected by the First Amendment.[41] This is based on the belief that debates on public matters should be protected, even if such debates devolve into offensive or hateful speech.[42]

3.3 In general, the requirements of the First Amendment to preserve "an uninhibited marketplace of ideas" apply against government actions rather than private actions.[43] In other words, the actions of individuals/private entities are not constrained by the First Amendment. In the digital environment where OSPs often play a role in hosting user-generated content, legislation is required to clarify whether online intermediaries are accountable for infringing content on their platforms.

Regulation of online speech and content

3.4 In the US, the **intermediary liability** of OSPs became an issue of concern when the Internet was still in its nascent stages. In the 1990s, the US courts handed down two contrasting cases on whether online forums were liable for defamatory content posted by its users. The first case held that online forums were not liable as long as they did not moderate any content on their platforms; whereas the second case held that online forums were liable if some content moderation was carried out.[44] Taken together, the two cases would have led to a "moderator's dilemma" where OSPs choose to avoid liability by not moderating any user-generated content on their platforms.[45]

3.5 In response to the two court cases, the Communications Decency Act ("CDA") was enacted in 1996 to clarify the role of OSPs in content moderation and ensure that online speech is not subject to undue restrictions. Under Section 230 of CDA, two related clauses of exemption are provided to OSPs for third-party content on their platforms. Specifically, the **first clause** states that OSPs are not liable for transmitting or hosting user-generated content,

---

41 Hate speech may be restricted if it becomes incitement, i.e. speech that is directed to, and likely causes, an immediate risk of a breach of peace. See Cornell Law School (1969).

42 See American Library Association (2017).

43 Private entities are only required to abide by the First Amendment in very limited circumstances. For instance, a private entity may be bound if it exercises "powers traditionally exclusively reserved to the state". See Congressional Research Service (2019b).

44 The cases are Cubby v CompuServe and Stratton Oakmont v Prodigy Services respectively. See Electronic Frontier Foundation (2020).

45 See US Department of Justice (2020).

provided that they have not materially contributed[46] to the content concerned. The **second clause** states that OSPs are not liable for moderating or removing objectionable material such as obscenity and violence posted by its users, as long as such actions are voluntary and taken in good faith[47].

3.6 The two exemption clauses resolve the "moderator's dilemma" by clarifying that OSPs are generally not liable for third-party content on their services. Furthermore, the clauses permit OSPs to regulate user-generated content on their own,[48] but **do not require active monitoring** of illegal content. Nevertheless, OSPs may still be required by other relevant laws to remove specific types of content, such as copyright infringements and material in violation of federal sex trafficking laws.[49]

Copyright infringements

3.7 In the US, the liability for copyright infringements is separately regulated by the Digital Millennium Copyright Act ("DMCA"), which was enacted in 1998 to incentivize OSPs and rights holders to cooperate against copyright violations. DMCA sets out a "safe harbour" regime under which OSPs are not liable for copyright infringements as long as they establish effective "notice-and-takedown" procedures, possess no prior knowledge of infringing activities, and promptly remove content when a copyright owner submits a valid notice. In general, a notice is valid if it (a) authenticates the rights holder; (b) identifies the copyright work and alleged infringement; and (c) states that the information provided is accurate and there is a good faith belief in infringement.[50]

3.8 In order to uphold the legitimate use of copyright material[51], the content uploader may contest the removal decision by filing a counter notice. Upon receiving a counter notice, the OSP must inform the copyright holder

---

[46] OSPs' ability to control the content that others post on its website is not considered as content creation. See Congressional Research Service (2019b).

[47] For instance, an OSP may not be acting in good faith if it selectively enforces a stated policy on its platform. See Congressional Research Service (2019b).

[48] In the US, major OSPs generally have in place self-regulatory community standards and/or content moderation policies to guide their implementation of content removal.

[49] Section 230 of CDA does not affect the enforcement of federal criminal laws.

[50] The notice requirements are by and large similar to the "notice-and-takedown" procedure proposed by the Copyright (Amendment) Bill 2014 in Hong Kong.

[51] The material removed might be a result of mistake or misidentification. The use of copyright material for criticism, news reporting, or research may be legal if it satisfies conditions of fair use.

and, if the rights holder decides not to file a lawsuit, restore the original content within 10 to 14 days.[52]

Protection of online data privacy

3.9 Unlike many overseas jurisdictions, the US does not have an overarching law on data privacy protection. Instead, several federal laws are in place to regulate the data protection practices of specific industries such as financial institutions and healthcare entities[53]. As a way to address this regulatory gap, the Federal Trade Commission[54] ("FTC") is empowered to investigate and prevent unfair or deceptive data practices.[55] FTC's enforcement actions[56] illustrate the data privacy standards which private companies including OSPs are expected to provide to their users. In particular, OSPs are expected to (a) provide sufficient information on the collection, use and disclosure of personal data; (b) abide by their own data privacy and security policies; and (c) employ security measures to protect the personal data of its consumers.

3.10 Over the years, FTC has brought enforcement actions against a number of major OSPs. For instance, a complaint was filed in 2019 against the social media platform Facebook for deceptive tactics to share users' personal data with third-party applications. As part of the settlement, Facebook is required to exercise greater oversight on third-party applications and its use of facial recognition technology. An independent third-party assessor is also appointed to evaluate and identify gaps in Facebook's privacy safeguards for personal data.[57]

---

[52] Further discussions of "notice-and-takedown" may be found in paragraphs 3.13 to 3.15.

[53] For example, the Right to Financial Privacy Act of 1978 establishes procedures that federal government authorities must follow to obtain information from a financial institution about a customer's financial records.

[54] FTC is a federal law enforcement agency responsible for protecting consumers and promoting competition across broad sectors of the economy. See Federal Trade Commission (2020a).

[55] The remit of FTC does not include non-profit organizations, federal credit unions, or financial institutions. See Cornell Law School (2012).

[56] As at 2017, FTC has brought over 500 enforcement actions against unfair or deceptive data practices. See Congressional Research Service (2020).

[57] See Federal Trade Commission (2019).

Issues on Internet freedom and regulation

3.11 In the US, the freedoms of expression and information, and to a lesser extent the right to privacy of Internet users, are protected by the US Constitution and a number of federal statutes. Yet, there are a number of outstanding issues regarding the regulatory regimes mentioned above which might affect the extent of freedom enjoyed by Internet users in the US.

Overbroad protections to OSPs

3.12 Section 230 of CDA has been credited as a key piece of legislation for free speech on the Internet[58]. It clarifies the legal liability of OSPs, shields them from what their users say, and permits them to moderate content on their platforms[59]. Yet, given the markedly different role played by online intermediaries since CDA was first enacted in 1996, others have questioned whether Section 230 has afforded overbroad protections to OSPs. For instance, there are views that Section 230 does not hold OSPs accountable for their content regulation policies. It is suggested that the lack of transparency requirements may open the door for OSPs to selectively enforce their content moderation policies.[60, 61]

Implementation of "notice-and-takedown"

3.13 Since its inception, DMCA's "notice-and-takedown" mechanism has seen wide adoption in the US and some overseas places.[62] The legislation has been commended for enabling access to information online,[63] since it limits

---

58 See American Civil Liberties Union (2019).

59 See Article 19 (2020).

60 See Department of Justice (2020) and Congressional Research Service (2019c).

61 On 28 May 2020, US President Donald Trump signed an Executive Order directing the Attorney General to develop a proposal for federal legislation to clarify the scope of Section 230 of CDA. On 17 June 2020, the Department of Justice put forth its initial proposals to restrict Section 230 immunity for (a) content related to child abuse, terrorism and cyber-stalking; (b) civil enforcement actions brought by the federal government; and (c) content moderation decisions that are not made according to a proposed statutory definition of good faith. See White House (2020) and US Department of Justice (2020).

62 Beyond the US, the "notice-and-takedown" mechanism has also been adopted by countries such as Australia, Singapore and South Korea.

63 See Electronic Frontier Foundation (2020).

the risk of copyright liability for OSPs and thereby incentivizes them to host user-generated content.

3.14 Yet, the implementation of "notice-and-takedown" has undergone some changes over the years. The expanding scale of online infringements has prompted some copyright holders to adopt automated systems to detect infringing content and submit notices. This has exponentially increased the number of notices received by OSPs, inducing some of them to sacrifice human review and deploy their own automated methods. According to an academic study, nearly one third of automated takedown notices were of questionable validity, and one in 25 apparently targeted the wrong material entirely.[64]

3.15 In light of these developments, Internet users have expressed concern over the accuracy and accountability of the "notice-and-takedown" regime. Despite the number of inaccurate notices, rights holders are seldom held liable for submitting mistaken information.[65] At the same time, content uploaders have reportedly made rare use of counter notices, giving rise to concerns that they lack effective redress to prevent the removal of legitimate content. This is mainly because individual users have relatively limited resource and capacity for legal action against, or in response to, the copyright holders.[66]

Lack of comprehensive data privacy protection

3.16 In the US, the current patchwork of federal data protection laws is limited to specific industries, specific types of data, and data practices that are unfair or deceptive. While FTC affords some general data protection for consumers, its enforcement repertoire is limited[67] and lacks jurisdiction over certain entities such as banks, insurance companies, and non-profit organizations. This has led to suggestions that more comprehensive data protection should be provided at the federal level.[68]

---

64 See Urban et al. (2016).

65 Under DMCA, parties submitting notices or counter notices must, under penalty of perjury, state that the information provided is accurate. See Wilson (2010).

66 See Urban et al. (2016).

67 Similar to the PCPD in Hong Kong, FTC cannot issue fines for first-time offences. Most enforcement actions by FTC result in companies entering into consent decrees requiring them to prevent further violations. Repeated contravention of the consent decrees may result in fines and/or further remedial actions. See Congressional Research Service (2019a) and AWSJ (2019).

68 See Council on Foreign Relations (2018) and Federal Trade Commission (2020b).

4. Internet freedom in the European Union

4.1 In the EU, the right to privacy and freedoms of expression and information are protected by Articles 8 and 10 of the European Convention on Human Rights ("ECHR"[69]) respectively[70, 71]. According to the Council of Europe, the two Articles deserve equal respect and the rights stated in ECHR apply equally in online and offline situations.[72] EU Member States have a duty to provide oversight on the exercise of right to freedoms of expression and information on the Internet, and to ensure that Internet users have access to effective remedies if their rights are harmed. Nevertheless, the rights of Internet users must also be weighed against other legitimate aims, such as the interests of national security or public safety, prevention of disorder or crime, and protection of the reputation or rights of others.

Regulation of online speech and content

4.2 In the EU, the **intermediary liability** of OSPs is laid out in the e-Commerce Directive, which was adopted in 2000 to facilitate cross-border online services in the EU. The Directive provides a "liability safe harbour" to incentivize OSPs to moderate user-generated content. Under the regime, OSPs are not liable for illegal content on their platforms, provided that they act expeditiously to remove or disable access to the infringing content upon receiving a relevant notice[73]. Furthermore, the Directive specifies that OSPs should **not be required to actively monitor** their platforms for illegal material[74].

---

69 ECHR is drafted by the Council of Europe. As Europe's leading human rights organization, the Council of Europe is comprised of 47 member states, 27 of which are EU Member States.

70 Article 8 of ECHR provides a right to respect for one's private life, whereas Article 10 provides the right to freedom of expression and information. Both articles are subject to certain restrictions that are "in accordance with the law" and "necessary in a democratic society".

71 The freedoms of expression and information and right to privacy are also protected by Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union. The Charter is drafted by the EU and is interpreted by the Court of Justice of the European Union.

72 See Council of Europe (2014).

73 In contrast to the US regime, the EU laws do not spell out the requirements for a valid notice.

74 Article 15 of the e-Commerce Directive prohibits EU Member States from imposing a general obligation on OSPs to monitor the information hosted to verify its legality. Yet, this does not mean that monitoring obligations cannot be imposed for specific cases. For example, Member States may require OSPs to inform the authorities of specific types of illegal activities upon obtaining the relevant knowledge. See EUR-Lex (2000).

4.3 The EU regime's "notice-and-takedown" applies to **all types of** illegal information, in contrast to the US regime which only applies to copyright infringements. However, the e-Commerce Directive does not spell out how OSPs ought to handle notices and takedowns, nor does it expressly provide procedural safeguards for Internet users affected by content removal. The European Commission, the executive arm of the EU, recognizes that this has resulted in a fragmented landscape with legal uncertainty for OSPs.[75] In response, it has gradually strengthened the intermediary liability regime of OSPs by introducing specific EU-wide legislation and voluntary codes and practices to tackle illegal content online.

4.4 In January 2020, the European Commission announced plans to revamp the e-Commerce Directive through the proposed Digital Services Act.[76] Specifically, the "notice-and-takedown" procedure would be replaced by an **EU-wide "notice-and-action" regime**, which provides more robust safeguards against illegal online content, with enforceable obligations on the complaint procedure, notice format, and response timeframes. Among other things, the proposed "notice-and-action" mechanism would:

(a) specify the requirements necessary to ensure that notices submitted are of good quality, thereby enabling a swift removal of illegal content;

(b) guarantee that notices would not automatically trigger the removal of specific pieces of content;

(c) require OSPs to verify the alleged infringing content and reply to the notice provider and content uploader, with clear justifications regarding the follow-up actions taken on the content concerned; and

---

[75] Member States have set up different systems including a "notice-and-takedown" system (i.e. the illegal content must be removed), a "notice and stay down" system (i.e. the illegal content must be removed and cannot be re-uploaded), or a "notice and notice system" (i.e. the OSP is only supposed to forward the notification of infringement to the alleged infringer). This heterogeneity of models across the EU has resulted in great legal uncertainty for OSPs. See European Parliamentary Research Service (2020).

[76] EC has initiated a public consultation on the Digital Services Act, which is open until 8 September 2020. The Act will be put forth in the last quarter of 2020. See European Parliament (2020b).

(d) provide all interested parties with the right to contest the decision through counter notices and by having recourse to out-of-court dispute settlement.

Copyright infringements

4.5 The regulation of online copyright material was previously governed by the e-Commerce Directive, where the liability of OSPs would be limited if they administer a "notice-and-takedown" scheme to expeditiously remove infringing content on their platforms. However, with the adoption of the Copyright Directive in April 2019,[77] OSPs are subject to a new regulatory regime and has to meet a number of "best efforts" requirements to protect copyright content.

4.6 In the first instance, OSPs should obtain **licences** from copyright holders to host and disseminate copyright works on their platforms. In cases where OSPs are unable to secure a licence, they are required to undertake further actions to avoid liability. In particular, they will need to demonstrate "best efforts" to (a) obtain an authorization from copyright holders; (b) ensure that content flagged by rights holders are made unavailable on their platforms; and (c) expeditiously remove and prevent the future upload of infringing content upon receiving a notice.[78, 79] According to the European Commission, the "best efforts" provision is a technology neutral requirement that should be met in accordance with "high industry standards of professional diligence". For instance, a major video-sharing platform has implemented an upload filter system which scans uploaded videos against a database of files submitted by rights holders. Videos flagged by the filter system may be removed from public access.[80]

---

[77] Member States have two years to implement the Copyright Directive via national legislation. See EUR-Lex (2019).

[78] The Directive exempts new OSPs which have provided services for less than three years and with annual turnover below €10 million (HK$88 million). It also excludes some OSPs such as open source sharing-platforms and cloud services that allow users to upload content for their own use.

[79] OSPs should provide redress mechanisms to prevent undue restrictions on the rights of users.

[80] Instead of direct removal, copyright holders may also choose to track the viewership statistics of the video, or monetize the video by running advertisements against it. See Youtube (2020).

Hate speech and disinformation

4.7 The EU has in recent years enhanced self-regulation of illegal hate speech[81] and disinformation in partnership with major OSPs such as Facebook, Google and Twitter.[82] **Illegal hate speech** is defined as expressions that incite violence or hatred directed against a group of persons defined by reference to race, colour, religion, descent or national or ethnic origin.[83] In 2016, the European Commission agreed on the *Code of Conduct on Countering Illegal Hate Speech Online* with a number of major OSPs committing to mitigate the harms of online hate speech.

4.8 The commitments as specified in the Code include the implementation of an effective removal process, a service pledge to respond to hate speech notices within 24 hours, and measures to certify civil society organizations as "trusted flaggers"[84] to submit credible notices on hate speech. Since 2018, the Code has been adopted by 96% of the EU market share of online platforms that may be affected by hate speech. This reportedly enhanced OSPs' responsiveness to the removal of hate speech on their platforms.[85]

4.9 In 2018, a number of major OSPs further agreed on a self-regulatory *Code of Practice on Disinformation* to tackle online **disinformation**.[86] Signatories to the Code have agreed to (a) ensure transparency of political and issue-based advertising; (b) intensify efforts to close fake accounts; (c) adopt technological means to prioritize relevant, authentic and accurate information; and (d) implement policies against misrepresentation.

4.10 In order to balance Internet users' right to information, the Code defines disinformation narrowly as those "verifiably false or misleading information" which may cause public harm, and is disseminated for economic gain or to intentionally deceive the public. The notion of "disinformation" does not include misleading advertisements, reporting errors, satire and

---

81 This contrasts with the US where hate speech is generally protected by the First Amendment.

82 The major OSPs agree to deliver their commitments voluntarily and on their own platforms. They also agree to self-assess, on a regular basis, whether these commitments have been met.

83 See European Commission (2016).

84 Trusted flaggers are trained personnel who can submit independent and credible notices.

85 For instance, the rate of hate speech notices reviewed within 24 hours increased from 40% in 2016 to 89% in 2019. OSPs have also recorded varying rates of content removal depending on the severity and type of hate speech reported. This suggests that OSPs assess the content with due care and regard for the freedom of expression. See European Commission (2019b).

86 See European Commission (2018).

parody, or clearly identified partisan news and commentary. In other words, signatories to the Code should not be compelled by governments nor adopt voluntary policies to prevent access to otherwise lawful material solely on the basis that they are thought to be "false"[87].

Protection of online data privacy

4.11 The EU has historically provided a privacy regime under the Data Protection Directive[88]. In May 2018, the new EU-wide General Data Protection Regulation ("GDPR") came into effect, imposing enhanced data security and governance requirements on data controllers[89], and providing data subjects with greater control over their personal data. Furthermore, GDPR is technology neutral and applicable to both governments and the private sector.[90, 91]

4.12 Recognizing that some kinds of data and types of processing may have more profound effects on private life, GDPR adopts a **risk-based approach** with measures to mitigate the privacy risks involved.[92] To begin with, OSPs are required to conduct prior **impact assessments** of any processing activities which could entail a high risk to the rights and freedoms of individuals. According to GDPR, examples of high risk processing include (a) systematic and extensive evaluation of individuals based on automated processing; and (b) large-scale processing of sensitive personal data[93]. The impact assessment should include descriptions of the processing operations, a risk assessment, and the proposed mitigation measures.[94]

---

87 See European Commission (2019a).

88 Reference was made to the Directive during the drafting of PDPO. See Wong (2018).

89 A data controller is defined as the entity which, alone or jointly with others, determines the purposes and means of the processing of personal data.

90 The rights of data subjects may be restricted in exceptional circumstances for the purposes of, among others, national security, defence, public security and the prevention or investigation of criminal offences. See EUR-Lex (2016).

91 GDPR covers the controllers/processors of EU data subjects' personal data, regardless of where the processing takes place. See EUR-Lex (2016).

92 See Data Protection Commission (Undated).

93 GDPR defines sensitive personal data as data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation". See EUR-Lex (2016).

94 If the impact assessment indicates that the processing activity is of high risk, the data controller is required to consult the relevant national data protection authorities. See EUR-Lex (2016).

4.13 Apart from impact assessments, GDPR affords some additional protection for persons subject to high risk processing. For instance, those who are subject to **automated decision-making** have a right to contest the decision and request human intervention from the data controller. On the other hand, **sensitive personal data** can only be processed (a) for prescribed purposes such as employment, medical diagnosis, and reasons in the public interest; or (b) with the explicit consent[95] of the data subject. As a last resort, data subjects can exercise control over their own data by requesting OSPs to remove data that is no longer necessary or relevant to the original purpose of collection. However, this **right to erasure** is not absolute and OSPs may reject the requests if there are overriding reasons for legal compliance or in the public interest.

4.14 GDPR also provides measures to ensure that **international data transfer**[96] does not compromise the protection of data subjects in the EU. Specifically, international data transfer can only occur when (a) the European Commission issues an "adequacy decision" attesting that a third country offers data protection that is on par with the EU;[97] or (b) other specific safeguards or conditions[98] are met. In order to ease the cost of compliance, the European Commission has issued standard contractual clauses to facilitate data transfer between businesses.

4.15 A data subject who considers his or her rights infringed may lodge a complaint with a national data protection authority. According to the European Data Protection Board, there has been an overall increase in data privacy complaints received since GDPR took effect.[99] As at 8 June 2020, there were a total of 282 reported cases of administrative fines imposed by the EU data protection authorities. Within the total, 48% were related to violations for insufficient legal basis for data processing and insufficient fulfilment of data subject rights.[100]

---

[95] Explicit consent refers to an express statement of consent which has a higher standard than the regular type of consent under GDPR. Examples of explicit consent include written or oral statements. See European Data Protection Board (2020).

[96] This refers to the transfer of personal data to countries outside the EU.

[97] EC has hitherto issued adequacy decisions for 13 countries including Canada, Japan, New Zealand and the US. Transfer of data from the EU to the US is limited to companies which have joined the EU-US Privacy Shield. See Privacy Shield Framework (2020).

[98] International data transfers can also take place if the transfer is necessary for the performance of a contract, or with the data subject's explicit consent. See EUR-Lex (2016).

[99] See European Data Protection Board (2019).

[100] See GDPR Enforcement Tracker (2020).

Issues on Internet freedom and regulation

4.16 In the EU, the right to privacy and freedoms of expression and information are protected with equal respect. Reflecting this, the EU has in recent years revamped its regulatory framework for illegal online content and implemented a more robust data protection regime. Nevertheless, there are still some discussions as to whether the regulatory developments outlined above would affect the extent of freedom enjoyed by Internet users in the EU.

Scope of the Digital Services Act

4.17 The proposed Digital Services Act has engendered some discussions regarding the future direction of the EU intermediary liability regime. In particular, there has been some debate on whether the Act should introduce binding provisions on "legal but harmful content" which is currently subject to self-regulation by OSPs.[101] For some, the moderation of "legal but harmful" content is conducive to a fair digital ecosystem and will not infringe the freedom of expression as long as the measures adopted are proportionate. Yet, there are also views that "harmful" content is highly contextual and hard to define, rendering such regulations difficult to enforce and prone to abuse.[102]

Use of preemptive technologies in content moderation

4.18 The Copyright Directive has generated widespread concern as to its effect on online speech. In order to avoid liability and follow the "best efforts" requirements, OSPs may have to impose upload filters to moderate their platforms.[103] The use of such preemptive technologies could lead to censorship of user-generated content at the point of upload, thereby affecting the freedom of expression online. In May 2019, the Polish government filed an application to the Court of Justice of the European Union seeking to annul the "best efforts" provisions of the Copyright Directive. The case is currently being considered by the court.[104]

---

[101] See European Parliament (2020a).

[102] See Article 19 (2020) and Center for Data Innovation (2020).

[103] Concerns have been raised by, among others, the United Nations Special Rapporteur on Freedom of Expression. See Infojustice (2019), Spoerri (2019) and United Nations (2019).

[104] See InfoCuria (2019).

Balance between data rights and access to information

4.19 Since its inception, there have been views that the GDPR's data rights could be abused to the detriment of other Internet freedoms. Specifically, the right to erasure requests may be targeted at search platforms or news websites [105], which could affect the freedom of press and access to information. Nevertheless, the right to erasure is not absolute[106] and OSPs may reject a request on grounds of public interest. According to a search engine, it has only complied with about 50% of all delisting requests made since GDPR came into effect on 25 May 2018.[107] Moreover, the delisting rate varied according to the type of requests, with a higher rate for sensitive personal information (94%) and lower rates for criminal content (60%) and political content (6%). The figures may reflect some degree of gatekeeping by OSPs based on the nature and validity of the requests raised by the data subjects concerned.

5. Concluding remarks

5.1 The Internet has evolved into a predominant and multi-faceted marketplace of ideas over the years. In accordance with international human rights instruments, the freedoms of expression and information that people enjoy offline are equally protected online. Yet, the Internet is unique insofar as its communications primarily take place via OSPs, i.e. online intermediaries where users contribute their content and provide their personal data. This has engendered discussions on whether regulatory regimes should hold OSPs accountable for moderating illicit online content such as copyright infringements or hate speech, while ensuring that the freedom of expression is also respected. With the increased scale and frequency of online data processing, there are also discussions on whether data rights should be enhanced to protect data subjects from the privacy risks involved.

---

[105] For instance, a person who had previously committed a crime may object to elements of his or her criminal past being disclosed to the public, e.g. through demanding all reference to the matter be expunged from newspaper archives.

[106] The Court of Justice of the European Union recently ruled that the right to erasure cannot be applied outside the EU, and that the right to freedom of expression must be weighed carefully before deleting links related to personal data. See The New York Times (2019).

[107] See Google Transparency Report (2020).

5.2 In Hong Kong, there has been no restriction to Internet access, and online censorship had not previously been an issue until recent months. Deliberations on OSP liability first emerged when the Government introduced the Copyright (Amendment) Bill 2014. In particular, copyright holders and OSPs saw the proposed "notice-and-takedown" as a clear and efficient mechanism to tackle copyright infringements without the need for court proceedings. However, some Internet users had concerns with its implementation and limited due process safeguards, and the amendment bill had since lapsed. In October 2019, the issue of OSP liability was again considered when the court granted an interim injunction against the incitement of the use or threat of violence online. In this case, the court stated that there is no positive duty on OSPs to search for or filter out unlawful content uploaded by its users.

5.3 The US and the EU have legislated on the duties and responsibilities of OSPs in moderating online content and protecting personal data privacy. In general, OSPs are not required to actively monitor their platforms for illicit material. As regards the intermediary liability regime, the US provides two broad exemption clauses to OSPs. The two clauses state that OSPs are generally not liable for third-party content on their platforms and moderating such content according to their own policies. Nevertheless, copyright infringement is a notable exception[108] as OSPs may be liable for infringing activities on their platforms, unless they abide by the "notice-and-takedown" procedure to remove the material upon receiving a valid notice.

5.4 Unlike the US, the EU has imposed a more restrictive intermediary liability regime. Although OSPs do not need to actively monitor their platforms for illegal material, they are required under the e-Commerce Directive to expeditiously remove **any illegal content** posted on their platforms upon receiving notice. In recent years, specific EU-wide laws and voluntary codes of practices have also been introduced to tackle copyright infringements, illegal hate speech and disinformation. In January 2020, the European Commission proposed its latest reform of the EU intermediary liability regime for OSPs. Under the proposed Digital Services Act, notices alone would not automatically trigger content removal. Instead, OSPs are obliged to verify the complaints, and reply to the parties involved with clear justifications for the follow-up actions taken.

[108] Section 230 of CDA also does not affect the enforcement of federal criminal laws.

5.5 In Hong Kong, PDPO regulates the collection, use, and disclosure of personal data. Amid the increased frequency in online data processing, there have been discussions on whether data rights should be enhanced to offer more protection for high risk processing. These include the handling of sensitive personal data (e.g. political opinions and biometrics), risk from new data processing technologies (e.g. automated decision making), and enforcement of the cross-border data transfer clause under Section 33 of PDPO.

5.6 The US and the EU have implemented contrastive data privacy protection regimes. The US has a patchwork of federal laws in place to regulate specific types of data. In contrast, the EU has in place an overarching data protection regime. **GDPR** is a technology neutral legislation with **risk-based measures** which are proportionate to the type of data processing involved. OSPs are required to conduct impact assessments before carrying out high risk processing such as automated decision-making. Data subjects also have some means to restrict OSPs' processing of their personal data, e.g. through the right to contest automated decision-making. Furthermore, the international transfer of data is limited to third countries with comparable levels of data protection or other appropriate safeguards.

5.7 In striving to define the role of OSPs in moderating online content, protecting personal data, and promoting the freedom of expression and access to information, the regulatory regimes in the US and the EU leave some room for concern in the following areas:

(a) the EU's proposed Digital Services Act has engendered concerns as to whether "legal but harmful content" would be regulated. While some are in support of proportionate measures to mitigate online harms, others have pointed out that "harmful" content is highly contextual, rendering any such regulations difficult to enforce and prone to abuse;

(b) OSPs hold discretion in deciding how to moderate illegal content on their platforms. In the US, some lawmakers have taken issue with CDA's overbroad protections and lack of transparency requirements on OSPs' content moderation policies. In the EU, OSPs may be motivated to adopt filters to remove infringing material at the point of upload in order to avoid liability for copyright infringements on their platforms;

(c) there are some concerns that the "notice-and-takedown" implemented in the US may lack effective redress to prevent removal of legitimate content. Although Internet users may submit counter notices, its actual usage has reportedly been low. Some content uploaders are deterred from submitting counter notices because of their relatively limited capacity to respond to legal actions by copyright holders; and

(d) the rights of some data subjects may adversely impact the access to information of other Internet users. For instance, requests to erase personal data may be targeted at news items or other public material. Granting these requests imply the precedence of the right to erasure over the public's right to access information online. In this regard, whether and how individual data rights are balanced against the public interest often depends on the gatekeeping efforts of the OSPs concerned.

Prepared by Charlie LAM
Research Office
Information Services Division
Legislative Council Secretariat
16 July 2020
Tel: 2871 2146

Internet freedom and content regulation in Hong Kong, the United States and the European Union

	Hong Kong	The United States ("US")	The European Union ("EU")
A. Legal basis for the freedom of expression online			
Legal basis	• Article 27 of the Basic Law; and • Article 16 of the Hong Kong Bill of Rights Ordinance ("HKBRO") (Cap. 383).	• First Amendment to the US Constitution.	• Article 10 of the European Convention on Human Rights; and • Article 11 of the Charter of Fundamental Rights of the European Union.
Whether online speech is also protected	• Yes. • HKBRO specifies that the freedom of expression applies regardless of frontiers or media.	• Yes. • The US Supreme Court has held that online speech is protected by the First Amendment.	• Yes. • The Council of Europe has stated that the freedom of expression applies equally to online and offline situations.
Legitimate restrictions	• Free speech may be subject to lawful restrictions that are necessary for: (a) respect of the rights or reputations of others; or (b) the protection of national security or of public order, or of public health or morals.	• Different categories of speech are afforded varying degrees of protection. • The government may regulate some categories of unprotected speech, such as obscenity, defamation, fraud and incitement.	• Free speech may be subject to lawful restrictions that are necessary for the interests of national security or public safety, prevention of disorder or crime and/or protection of the reputation or rights of others.

Internet freedom and content regulation in Hong Kong, the United States and the European Union

	Hong Kong	The United States ("US")	The European Union ("EU")
B. Regulation of online speech and content			
Any specific provisions on intermediary liability of OSPs	• No.	• Yes. • Section 230 of the Communications Decency Act provides two exemption clauses. The first clause states that OSPs are generally not liable for third-party content on their platforms. The second clause permits OSPs to regulate user-generated content on their own. OSPs are not required to actively monitor their platforms for illegal content. • The exemptions afforded by Section 230 does not apply to (a) federal criminal laws; (b) copyright laws; and (c) material which violates federal laws against sex trafficking.	• Yes. • The e-Commerce Directive provides a "liability safe harbour" where OSPs are not liable for illegal content on their platforms, as long as they expeditiously remove any infringing content upon receiving a relevant notice. • OSPs should not be required by EU Member states to actively monitor their platforms for illegal activity.
Any regulation of online copyright content	• Yes. • The Copyright Ordinance (Cap. 528) affords civil remedies and criminal sanctions against content which infringes the copyright owners' right to copy or distribute their work.	• Yes. • The Digital Millennium Copyright Act provides "safe harbour" provisions to limit the liability of OSPs for copyright infringement on their platforms.	• Yes. • The Copyright Directive specifies additional duties of care for OSPs for copyright infringement on their platforms.

Internet freedom and content regulation in Hong Kong, the United States and the European Union

	Hong Kong	The United States ("US")	The European Union ("EU")
B. Regulation of online speech and content (cont'd)			
Any regulation of online hate speech	• No. • The court has granted an interim injunction against the dissemination of material which incites the use or threat of violence online. However, there is no positive duty on OSPs to search for or filter out unlawful content uploaded by others.	• No. • Hate speech which demeans on the basis of race, ethnicity, or gender is protected by the First Amendment. • However, the government may regulate speech of incitement which is (a) directed to inciting or producing imminent lawless action; and (b) is likely to incite or produce such action.	• Yes. • The European Commission has agreed to a voluntary code of conduct with major OSPs to counter the spread of illegal hate speech online. • Illegal hate speech is defined as expressions which incite violence or hatred directed to groups or individuals on the basis of certain characteristics, including race, colour, religion, descent and national or ethnic origin.
Any regulation of disinformation	• No.	• No.	• Yes. • The European Commission has agreed to a voluntary code of practice with major OSPs to tackle online disinformation. • Disinformation is defined narrowly as information that is verifiably false or misleading, which may cause public harm and is disseminated for economic gain or to intentionally deceive the public.

Internet freedom and content regulation in Hong Kong, the United States and the European Union

	Hong Kong	The United States ("US")	The European Union ("EU")
C. Mandatory "notice-and-takedown" of online content by OSPs			
Scope of "notice-and-takedown"	• Not available.	• Copyright infringements only.	• All illegal content online, with additional requirements for copyright infringements.
Specified procedure for "notice-and-takedown"		• The procedure involves (a) submission of a proper notice from the copyright holder; (b) expeditious removal of the alleged infringing material by the OSP; and (c) notification of takedown by the OSP to the original uploader. • A valid notice should (a) authenticate the rights holder; (b) identify the copyright work and alleged infringement; and (c) state that the information provided is accurate.	• The e-Commerce Directive only requires that OSPs act expeditiously to remove or disable access to the illegal content, upon receiving a valid notice. • The Copyright Directive requires OSPs to obtain licences from rights holders for the use of their work. In lieu of a licence, OSPs must demonstrate best efforts to (a) obtain an authorization from copyright holders; (b) ensure that unauthorized content is not available on their platforms; and (c) expeditiously remove and prevent the future upload of infringing content upon receiving a notice.
Any measures to safeguard the freedom of expression		• Yes. • The original uploader may contest the takedown with a counter notice. Upon receiving a counter notice, the OSP must restore the content within 10 to 14 days unless the copyright holder files a lawsuit. • Parties submitting notices and counter notices must, under penalty of perjury, state that the information provided is accurate.	• Not generally available. • For copyright content, OSPs are required to put in place complaint and redress mechanisms to prevent undue restrictions on the rights of Internet users. • The European Commission plans to revamp the "notice-and-takedown" of illegal content through the Digital Services Act, so that notices alone would not automatically trigger content removal.

Internet freedom and privacy protection in Hong Kong, the United States and the European Union

	Hong Kong	The United States ("US")	The European Union ("EU")
A. Legal basis for the right to privacy			
Legal basis	• Article 30 of the Basic Law; and • Article 14 of HKBRO.	• The right to privacy is not expressly enshrined in the US Constitution. • Some provisions such as the Fourth and Fourteenth Amendments have been interpreted to protect personal privacy.	• Article 8 of the European Convention on Human Rights; and • Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.
Any legislation on protection of personal data	• Yes. • Personal Data (Privacy) Ordinance ("PDPO") (Cap. 486).	• Yes. • A patchwork of federal laws is in place to regulate the data protection practices of specific industries such as financial institutions and healthcare entities. • The Federal Trade Commission Act ("FTCA") prohibits unfair or deceptive practices involving personal data of consumers.	• Yes. • General Data Protection Regulation ("GDPR").
Responsible authority	• Office of the Privacy Commissioner for Personal Data ("PCPD").	• Federal Trade Commission ("FTC").	• European Data Protection Board ("EDPB"); and • National data protection authorities of EU Member States.

Internet freedom and privacy protection in Hong Kong, the United States and the European Union

	Hong Kong	The United States ("US")	The European Union ("EU")
B. Measures to protect personal data			
Any data rights for Internet users	• Yes. • PDPO affords Internet users with the rights to request access to and correction of personal data.	• No. • Yet, FTC protects consumers by enforcing against companies which: (a) gather, use or disclose personal data in contradiction of their stated policies; (b) make false representations to induce the disclosure of personal data; and (c) fail to employ adequate measures to secure personal data.	• Yes. • GDPR affords Internet users with the following data rights: (a) right to be informed; (b) right of access; (c) right to rectification; (d) right to erasure; (e) right to restrict processing; (f) right to data portability; and (g) right to object.
Any regulation of cross-border data transfer	• Yes, Section 33 of PDPO specifies that personal data should not be transferred outside Hong Kong unless the overseas place is on PCPD's "white list" with similar data protection laws, or with the data subject's explicit consent. • However, Section 33 is not yet in force.	• No. • However, FTC administers the EU-US Privacy Shield which provides enforceable protections for the transfer of personal data from the EU to the US.	• Yes. • Articles 44 to 50 of GDPR specify that personal data can only be transferred to third countries when: (a) the European Commission issues an adequacy decision; or (b) appropriate safeguards such as standard contractual clauses are in place.

Internet freedom and privacy protection in Hong Kong, the United States and the European Union

	Hong Kong	The United States ("US")	The European Union ("EU")
B. Measures to protect personal data (cont'd)			
Any additional safeguards	• No.	• No. • FTC has brought a number of enforcement actions against major OSPs such as Facebook.	• Yes. • OSPs are required to conduct prior impact assessment of any processing activities that could entail a high risk to the rights and freedoms of individuals. • Internet users who are subject to automated decision-making have a right to contest the decision and obtain human intervention. • The processing of sensitive personal data such as political opinions or biometrics is subject to further restrictions.
Any exemptions	• Yes. • PDPO provides various exemptions for domestic purposes, employment, and news, statistics and research.	• Yes. • FTCA does not cover entities such as non-profit organizations.	• Yes. • GDPR does not apply to purely personal or household activities. Member states are required to provide exemptions for processing for journalistic purposes, and academic, artistic or literary expression.

References

Hong Kong

1. Cato Institute. (2019) *The Human Freedom Index 2019*. Available from: https://www.cato.org/sites/cato.org/files/human-freedom-index-files/cato-human-freedom-index-update-3.pdf [Accessed July 2020].

2. CLIC. (2018) *Intellectual Property*. Available from: https://www.clic.org.hk/en/topics/intellectualProperty/ [Accessed July 2020].

3. Commerce and Economic Development Bureau. (2014) *Legislative Council Brief of Copyright (Amendment) Bill 2014*. Available from: https://www.legco.gov.hk/yr13-14/english/bills/brief/b201406131_brf.pdf [Accessed July 2020].

4. Constitutional and Mainland Affairs Bureau. (2019) *Progress Report of Motion on "Keeping up with Technological Development and Enhancing the Protection of People's Privacy"*. Available from: https://www.legco.gov.hk/yr18-19/english/counmtg/motion/cm20190522m-lmf-prpt-e.pdf [Accessed July 2020].

5. Constitutional and Mainland Affairs Bureau. (2020) *Review of the Personal Data (Privacy) Ordinance*. LC Paper No. CB(2)512/19-20(03). Available from: https://www.legco.gov.hk/yr19%2D20/english/panels/ca/papers/ca20200120cb2-512-3-e.pdf [Accessed July 2020].

6. Freedom House. (2020) *Freedom in the World 2020: Hong Kong*. Available from: https://freedomhouse.org/country/hong-kong/freedom-world/2020 [Accessed July 2020].

7. GovHK. (2006) *Government seeks public views on strengthening copyright protection in digital environment*. Available from: https://www.info.gov.hk/gia/general/200612/19/P200612190205.htm [Accessed July 2020].

8. GovHK. (2019) *LCQ12: Requests made to ICT companies for disclosure and removal of information*. Available from: https://www.info.gov.hk/gia/general/201902/27/P2019022700291.htm [Accessed July 2020].

9. Hong Kong Bar Association. (2016) *Position Paper on Copyright (Amendment) Bill 2014 and the 3 Amendments Proposed by Certain LegCo Members*. Available from: https://www.hkba.org/sites/default/files/Copyright%20%28Amendment%29%20Bill%202014%20...%20%28E%29.pdf [Accessed July 2020].

10. Hong Kong e-Legislation. (2017) *Cap. 383 Hong Kong Bill of Rights Ordinance*. Available from: https://www.elegislation.gov.hk/hk/cap383 [Accessed July 2020].

11. Hong Kong Police Force. (2019) *Interim Injunction Order of the High Court (HCA 2007/2019)*. Available from: https://www.police.gov.hk/ppp_en/03_police_message/iio_202.html [Accessed July 2020].

12. Hong Kong Transparency Project. (2018) *2018 Transparency Report*. Available from: http://transparency.jmsc.hku.hk/wp%2Dcontent/uploads/2018/06/HongKongTransparencyReport2018_EN_V2.pdf [Accessed July 2020].

13. Human Rights Watch. (2020) *Re: Review of the Personal Data (Privacy) Ordinance*. LC Paper No. CB(2)548/19-20(01). Available from: https://www.legco.gov.hk/yr19%2D20/chinese/panels/ca/papers/ca20200120cb2-548-1-ec.pdf [Accessed July 2020].

14. Intellectual Property Department. (2014) *Copyright (Amendment) Bill 2014*. Available from: https://www.ipd.gov.hk/eng/intellectual_property/copyright/Keynote_2014_e.pdf [Accessed July 2020].

15. Intellectual Property Department. (2017) *Copyright (Amendment) Bill 2014: Frequently Asked Questions*. Available from: https://www.ipd.gov.hk/eng/intellectual_property/copyright/Q_A_2014.htm#q9 [Accessed July 2020].

16. Internet Society. (2019) *Internet Society Deeply Concerned about Interim Injunction Ordered by Hong Kong High Court*. Available from: https://www.internetsociety.org/news/statements/2019/interim-injunction-ordered-by-hong-kong-high-court/ [Accessed July 2020].

17. Internet Society Hong Kong. (2019a) *Court issued restrictions on the injunction of banning online free speech concerns over Internet censorship remained*. Available from: https://www.isoc.hk/news/網絡審查禁制令範圍收窄-關注政府繼續製造寒蟬效/ [Accessed July 2020].

18. Internet Society Hong Kong. (2019b) *Internet Society Hong Kong's Legal Challenge against Government's Injunction of Blocking Free Speech Online*. Available from: https://www.isoc.hk/news/jr-against-online-censorship/ [Accessed July 2020].

19. Legal Reference System. (2019) *HCA 2007/2019 Secretary for Justice v Persons Unlawfully and Wilfully Conducting Themselves in any of the Acts Prohibited under Paragraph 1(a) and (b) of the Indorsement of Claim*. Available from: https://legalref.judiciary.hk/lrs/common/search/search_result_detail_frame.jsp?DIS=125435&QS=%2B&TP=JU [Accessed July 2020].

20. Legislative Council Secretariat. (2020) *Background brief of Review of the Personal Data (Privacy) Ordinance.* LC Paper No. CB(2)512/19-20(04). Available from: https://www.legco.gov.hk/yr19%2D20/english/panels/ca/papers/ca20200120cb2-512-4-e.pdf [Accessed July 2020].

21. Motion Picture Association. (2014) *Written submissions to Bills Committee on Copyright (Amendment) Bill 2014*. LC Paper No. CB(4)67/14-15(08). Available from: https://www.legco.gov.hk/yr13%2D14/english/bc/bc106/papers/bc1061025cb4-67-8-e.pdf [Accessed July 2020].

22. Office of the Privacy Commissioner for Personal Data. (2014a) *Guidance for Data Users on the Collection and Use of Personal Data through the Internet*. Available from: https://www.pcpd.org.hk//english/resources_centre/publications/files/guidance_internet_e.pdf [Accessed July 2020].

23. Office of the Privacy Commissioner for Personal Data. (2014b) *Guidance on Personal Data Protection in Cross-border Data Transfer*. Available from: https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf [Accessed July 2020].

24. Office of the Privacy Commissioner for Personal Data. (2019) *Data Breach Incident Investigation Report: Cathay Pacific Airways Limited and Hong Kong Dragon Airlines Limited*. Available from: https://www.pcpd.org.hk/english/media/media_statements/files/PCPD_Investigation_Report_R19_15281_E.pdf [Accessed July 2020].

25. Review of the Control of Obscene and Indecent Articles Ordinance. (2020) *Frequently Asked Questions About the Existing Regulatory Regime*. Available from: https://www.coiao.gov.hk/en/faq.htm [Accessed July 2020].

26. US Department of State. (2019) *2019 Country Reports on Human Rights Practices: China (Includes Hong Kong, Macau, and Tibet) – Hong Kong*. Available from: https://www.state.gov/reports/2019-country-reports-on-human-rights-practices/china/hong-kong/ [Accessed July 2020].

27. 國際特赦組織香港分會：《國際特赦組織香港分會就《2014 年版權(修訂)條例草案》之意見書》，2014 年，立法會 CB(4)171/14-15(06) 號文件，網址：https://www.legco.gov.hk/yr13%2D14/chinese/bc/bc106/papers/bc1061025cb4-171-6-c.pdf [於 2020 年 7 月登入]。

The European Union

28. Article 19. (2020) *Article 19's Recommendations for the EU Digital Services Act*. Available from: https://www.article19.org/wp%2Dcontent/uploads/2020/04/ARTICLE-19s-Recommendations-for-the-EU-Digital-Services-Act-FINAL.pdf [Accessed July 2020].

29. Bird & Bird. (2019) *Personal data and freedom of expression*. Available from: https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression [Accessed July 2020].

30. Center for Data Innovation. (2020) *What the EU Should Put in the Digital Services Act*. Available from: http://www2.datainnovation.org/2020-eu-digital-services-act.pdf [Accessed July 2020].

31. Council of Europe. (2014) *Guide to Human Rights for Internet Users*. Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DOSPlayDCTMContent?documentId=09000016804d5b31 [Accessed July 2020].

32. Data Protection Commission. (Undated) *Risk based approach*. Available from: https://www.dataprotection.ie/en/organisations/know-your-obligations/risk-based-approach [Accessed July 2020].

33. EUR-Lex. (2000) *Directive 2000/31/EC*. Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031 [Accessed July 2020].

34. EUR-Lex. (2001) *Directive 2001/29/EC*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001L0029 [Accessed July 2020].

35. EUR-Lex. (2016) *Regulation (EU) 2016/679*. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed July 2020].

36. EUR-Lex. (2019) *Directive (EU) 2019/790*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0790 [Accessed July 2020].

37. European Commission. (2016) *The EU Code of conduct on countering illegal hate speech online*. Available from: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en#theeucodeofconduct [Accessed July 2020].

38. European Commission. (2018) *EU Code of Practice on Disinformation*. Available from: https://www.hadopi.fr/sites/default/files/sites/default/files/ckeditor_files/1CodeofPracticeonDisinformation.pdf [Accessed July 2020].

39. European Commission. (2019a) *Code of Practice on Disinformation one year on: online platforms submit self-assessment reports*. Available from: https://ec.europa.eu/commission/presscorner/detail/en/statement_19_6166 [Accessed July 2020].

40. European Commission. (2019b) *Fourth evaluation confirms self-regulation works*. Available from: https://ec.europa.eu/info/sites/info/files/code_of_conduct_factsheet_7_web.pdf [Accessed July 2020].

41. European Commission. (2019c) *Frequently Asked Questions on Copyright Reform*. Available from: https://ec.europa.eu/digital%2Dsingle%2Dmarket/en/faq/frequently-asked-questions-copyright-reform [Accessed July 2020].

42. European Commission. (2020) *Shaping the Digital Single Market*. Available from: https://ec.europa.eu/digital%2Dsingle%2Dmarket/en/policies/shaping-digital-single-market [Accessed July 2020].

43. European Data Protection Board. (2019) *1 Year GDPR – Taking Stock*. Available from: https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en [Accessed July 2020].

44. European Data Protection Board. (2020) *Guidelines 05/2020 on consent under Regulation 2016/679*. Available from: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf [Accessed July 2020].

45. European Parliament. (2020a) *Draft Report on the Digital Services Act and Fundamental Rights Issues Posed*. Available from: https://www.europarl.europa.eu/doceo/document/LIBE-PR-650509_EN.pdf [Accessed July 2020].

46. European Parliament. (2020b) *Draft Report with Recommendations to the Commission on Digital Services Act*. Available from: https://www.europarl.europa.eu/doceo/document/IMCO-PR-648474_EN.pdf [Accessed July 2020].

47. European Parliamentary Research Service. (2020) *Reform of the EU Liability Regime for Online Intermediaries*. Available from: https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_EN.pdf [Accessed July 2020].

48. *GDPR Enforcement Tracker*. (2020) Available from: https://www.enforcementtracker.com/? [Accessed July 2020].

49. *Google Transparency Report*. (2020) Available from: https://transparencyreport.google.com/ [Accessed July 2020].

50. InfoCuria. (2019) *Action brought on 24 May 2019 – Republic of Poland v European Parliament and Council of the European Union*. Available from: http://curia.europa.eu/juris/document/document.jsf?text=&docid=216823&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8371710 [Accessed July 2020].

51. Infojustice. (2019) *Concern grows over spread of EU copyright filtering rules*. Available from: http://infojustice.org/archives/41212 [Accessed July 2020].

52. Keller, D. (2017) *The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation*. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2914684 [Accessed July 2020].

53. Kuczerawy, A. (2017) *Intermediary Liability and the Effective Enjoyment of the Right to Freedom of Expression*. Available from: https://www.jipitec.eu/issues/jipitec-8-3-2017/4623/JIPITEC_8_3_2017_226_Kuczerawy [Accessed July 2020].

54. Reventlow, N. J. (2020) *Can the GDPR and Freedom of Expression Coexist?* Available from: https://www.cambridge.org/core/journals/american%2Djournal-of-international-law/article/can-the-gdpr-and-freedom-of-expression-coexist/C8C5B4F0BFF87B9CAD78ED4BDDF27BBC/core-reader [Accessed July 2020].

55. Spoerri, T. (2019) *On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market*. Available from: https://www.jipitec.eu/issues/jipitec-10-2-2019/4914 [Accessed July 2020].

56. The New York Times. (2019) *'Right to be forgotten' privacy rule is limited by Europe's top court*. Available from: https://www.nytimes.com/2019/09/24/technology/europe-google-right-to-be-forgotten.html [Accessed July 2020].

57. United Nations. (2019) *EU must align copyright reform with international human rights standards, says expert*. Available from: https://www.ohchr.org/EN/NewsEvents/Pages/DOSPlayNews.aspx?NewsID=24298&LangID=E [Accessed July 2020].

58. Wong, S.K.Y. (2018) *EU GDPR and HK PDPO: What's the Difference?* Available from: http://www.hk-lawyer.org/content/eu-gdpr-and-hk-pdpo-what%E2%80%99s-difference [Accessed July 2020].

59. Youtube. (2020) *How Content ID works*. Available from: https://support.google.com/youtube/answer/2797370?hl=en [Accessed July 2020].

The United States

60. American Civil Liberties Union. (2019) *Our Online Speech Rights are under Threat*. Available from: https://www.aclu.org/news/free-speech/our-online-speech-rights-are-under-threat/ [Accessed July 2020].

61. American Library Association. (2017) *Hate Speech and Hate Crime*. Available from: http://www.ala.org/advocacy/intfreedom/hate [Accessed July 2020].

62. Article 19. (2020) *US: Trump's Executive Order threatens freedom of expression online*. Available from: https://www.article19.org/resources/article-19-trumps-executive-order-threatens-freedom-expression-online/ [Accessed July 2020].

63. Brent. K. et al. (2019) Looming Facebook Fine Points to a Tougher Cop on the Tech Beat; The Federal Trade Commission is wrapping up its probe of Facebook's data-privacy protections—and could establish safeguards for social-media industry. *AWSJ*. 25 April.

64. Congressional Research Service. (2014) *Safe Harbor for Online Service Providers Under Section 512(c) of the Digital Millennium Copyright Act*. Available from: https://crsreports.congress.gov/product/pdf/R/R43436 [Accessed July 2020].

65. Congressional Research Service. (2019a) *Data Protection Law: An Overview*. Available from: https://crsreports.congress.gov/product/pdf/R/R45631 [Accessed July 2020].

66. Congressional Research Service. (2019b) *Free Speech and the Regulation of Social Media Content*. Available from: https://fas.org/sgp/crs/misc/R45650.pdf [Accessed July 2020].

67. Congressional Research Service. (2019c) *Liability for Content Hosts: An Overview of the Communication Decency Act's Section 230*. Available from: https://fas.org/sgp/crs/misc/LSB10306.pdf [Accessed July 2020].

68. Congressional Research Service. (2019d) *Regulating Big Tech: Legal Implications*. Available from: https://crsreports.congress.gov/product/pdf/LSB/LSB10309 [Accessed July 2020].

69. Congressional Research Service. (2019e) *The First Amendment: Categories of Speech*. Available from: https://fas.org/sgp/crs/misc/IF11072.pdf [Accessed July 2020].

70. Congressional Research Service. (2020) *Digital Millennium Copyright Act (DMCA) Safe Harbor Provisions for Online Service Providers: A Legal Overview*. Available from: https://crsreports.congress.gov/product/pdf/IF/IF11478 [Accessed July 2020].

71. Cornell Law School. (1969) *Brandenburg Test*. Available from: https://www.law.cornell.edu/wex/brandenburg_test [Accessed July 2020].

72. Cornell Law School. (2012) *15 U.S. Code §45*. Available from: https://www.law.cornell.edu/uscode/text/15/45 [Accessed July 2020].

73. Cornell Law School. (2018) *47 U.S. Code §230*. Available from: https://www.law.cornell.edu/uscode/text/47/230 [Accessed July 2020].

74. Council on Foreign Relations. (2018) *Reforming the US Approach to Data Protection and Privacy*. Available from: https://www.cfr.org/report/reforming-us-approach-data-protection [Accessed July 2020].

75. Electronic Frontier Foundation. (2020) *CDA 230: The Most Important Law Protecting Internet Speech*. Available from: https://www.eff.org/issues/cda230 [Accessed July 2020].

76. Federal Trade Commission. (2019) *FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook*. Available from: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [Accessed July 2020].

77. *Federal Trade Commission*. (2020a) Available from: https://www.ftc.gov/ [Accessed July 2020].

78. Federal Trade Commission. (2020b) *Privacy & Data Security Update for 2019*. Available from: https://www.ftc.gov/reports/privacy-data-security-update-2019 [Accessed July 2020].

79. Internet Association. (2017) *New Report Finds Weakened Intermediary Liability Protections will cost 4.25 Million Jobs and Nearly Half a Trillion Dollars in the Next Decade*. Available from: https://internetassociation.org/report-finds-weakened-intermediary-liability-protection-cost-4-25-million-jobs-and-nearly-half-a-trillion-dollars-in-the-next-decade/ [Accessed July 2020].

80. Leslie, A. (2017) *Digital Millennium Copyright Act (DMCA) Notice & Takedown Procedure*. Available from: https://www.hostingadvice.com/how-to/dmca-notice/ [Accessed July 2020].

81. *Privacy Shield Framework*. (2020) Available from: https://www.privacyshield.gov/welcome [Accessed July 2020].

82. Seltzer, W. (2010) *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*. Available from: https://wendy.seltzer.org/pubs/seltzer-chill.pdf [Accessed July 2020].

83. Stanford Law School. (2020) *Intermediary Liability*. Available from: http://cyberlaw.stanford.edu/focus-areas/intermediary-liability [Accessed July 2020].

84. Taruschio, A.M. (2000) The First Amendment, The Right Not To Speak And The Problem Of Government Access Statutes. *Fordham Urb. Law Journal*, vol. 7, no. 3, article 10. Available from: https://ir.lawnet.fordham.edu/ulj/vol27/iss3/10 [Accessed July 2020].

85. US Department of Justice. (2020) *Department of Justice's Review of Section 230 of the Communications Decency Act of 1996*. Available from: https://www.justice.gov/ag/department-justice-s-review-section-230-communications%2Ddecency%2Dact%2D1996?utm_medium=email&utm_source=govdelivery [Accessed July 2020].

86. US Department of State. (various years) *Country Reports on Human Rights Practices in China (Includes Hong Kong, Macau, and Tibet)*. Available from: https://www.state.gov/reports/2019-country-reports-on-human-rights-practices/china/hong-kong/ [Accessed July 2020].

87. Urban, J. M. et al. (2016) *Notice and Takedown in Everyday Practice*. Available from: http://illusionofmore.com/wp%2Dcontent/uploads/2016/04/Berkeley_Columbia-on-512-takedown.pdf [Accessed July 2020].

88. White House. (2020) *Executive Order on Preventing Online Censorship*. Available from: https://www.whitehouse.gov/presidential%2Dactions/executive-order-preventing-online-censorship/ [Accessed July 2020].

89. Wilson, Benjamin. (2010) Notice, Takedown, and the Good-Faith Standard: How to Protect Internet Users from Bad-Faith Removal of Web Content. *Saint Louis University Public Law Review*, vol. 29, no. 2, article 12. Available from: https://scholarship.law.slu.edu/cgi/viewcontent.cgi?article=1173&context=plr [Accessed July 2020].

Others

90. eshopworld. (2019) *Global Ecommerce Market Ranking 2019*. Available from: https://www.worldretailcongress.com/__media/Global_ecommerce_Market_Ranking_2019_001.pdf [Accessed July 2020].

91. Oberlo. (2019) *Ecommerce Sales by Country in 2019*. Available from: https://www.oberlo.com/statistics/ecommerce-sales-by-country [Accessed July 2020].

92. Organisation for Economic Co-operation and Development. (2010) *The Economic and Social Role of Internet Intermediaries*. Available from: https://www.oecd.org/internet/ieconomy/44949023.pdf [Accessed July 2020].

93. *Our World in Data*. (2019) Available from: https://ourworldindata.org/internet [Accessed July 2020].

94. The World Bank. (2019) *Individuals using the Internet (% of population).* Available from: https://data.worldbank.org/indicator/IT.NET.USER.ZS [Accessed July 2020].

95. United Nations. (1976) *International Covenant on Civil and Political Rights*. Available from: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx [Accessed July 2020].

96. United Nations. (2011) *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. Available from: https://undocs.org/en/A/HRC/17/27 [Accessed July 2020].

97. United Nations. (2016) *The promotion, protection and enjoyment of human rights on the Internet*. Available from: https://undocs.org/A/HRC/32/L.20 [Accessed July 2020].

98. United Nations Treaty Collection. (2020) *Status of Treaties*. Available from: https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en [Accessed July 2020].