2022

Revolt against the U.S. Hegemony: Judicial Divergence in Cyberspace

Dongsheng Zang
University of Washington School of Law

REVOLT AGAINST THE U.S. HEGEMONY: JUDICIAL DIVERGENCE IN CYBERSPACE

DONGSHENG ZANG*

---

* Associate Professor of Law, University of Washington School of Law. I would like to thank my colleague Professor Jennifer Fan, Professors Rikako Watai and David G. Litt of Keio University (Tokyo, Japan), Mr. Jesse Woo, for their helpful comments on earlier drafts of this Article. I benefited from speakers at the UW-Keio Conference on Open Access to Data and Innovation, February 25 and 26, 2021, including Professors Tatsuhiko Yamamoto, Mary Fan, Mr. Stephen Mortinger, Professor Ryan Calo, Mr. Jody Chafee, and Professor Tadayoshi Kohno. I also benefited from communications with Professors Daniel H. Foote and Shigenori Matsui. Special thanks to Ms. Cindy Fester for her earlier editorial assistance. In the summer and fall of 2021, I had the privilege and pleasure in working with a team of talented editorial staff at the *Wisconsin International Law Journal*—Natalie Riopelle, Justin Brewer, Peter Bazianos, Madison Wescott, Ola Lisowski, and Andrew Campbell—who offered me enormous assistance and excellent suggestions for improving the manuscript. Of course, all errors are mine.

INTRODUCTION

The internet is increasingly fragmented. In the summer of 2020, when then President Trump decided to block Chinese apps TikTok and WeChat by executive orders,[1] the *New York Times* warned that the Trump Administration's hardline policy on China "may split the web."[2] This warning echoes what former Google CEO Eric Schmidt was quoted as saying in September 2018—that in the next ten to fifteen years, the internet would most likely be split into two with one led by China and one led by the United States.[3] The Biden Administration repealed some measures taken by Trump,[4] but has not changed the fundamentally aggressive policy towards China.[5] China did not merely remain on the defensive. In 2021, two major pieces of legislation on cyberspace were passed—the Data Security Law (DSL), and the Personal Information Protection Law (PIPL).[6] These legislations reflected and consolidated a general

---

1 Two executive orders were issued by President Trump in August 2020: Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020) (relating to the TikTok app) and Exec. Order No. 13,943, 85 Fed. Reg. 48,637 (Aug. 6, 2020) (relating to WeChat). The executive order was quickly challenged, however, and a federal district court in California issued a nationwide injunction against implementation. *See* WeChat Users Alliance v. Trump, 488 F. Supp. 3d 912 (N.D. Cal. 2020), *appeal docketed*, No. 20-16908 (9th Cir. Oct. 2, 2020) (granting plaintiffs preliminary injunctive relief against implementation of Executive Order 13,943). On June 9, 2021, the Biden Administration revoked the ban on TikTok and WeChat. John D. McKinnon & Alex Leary, *Biden Revokes Bid to Ban TikTok, WeChat*, WALL ST. J., June 10, 2021, at A1.

2 Ana Swanson, Paul Mozur & Raymond Zhong, *U.S. Hard Line on China Tech May Split Web*, N.Y. TIMES, Aug. 18, 2020, at A1.

3 Editorial, *As Internet Splinters, the World Suffers*, N.Y. TIMES, Oct. 16, 2018, at A22.

4 *See* Dan Strumpf, *Pentagon Pulls Xiaomi off Sanctions List,* WALL ST. J., May 13, 2021, at B4.

5 *See* Bob Davis, *U.S. Eyes Tech Alliance Against China*, WALL ST. J., Mar. 1, 2021, at A2.

6 Zhonghua Renmin Gongheguo Shuju Anquan Fa (中华人民共和国数据安全法) [Data Security Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., June 10, 2021, effective Sept. 1, 2021), STANDING. COMM. NAT'L PEOPLE'S CONG. GAZ. 951 (2021); Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021), STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 1117 (2021).

framework characterized by data localization requirements and governmental scrutiny.

A split on the internet is happening across the Atlantic as well. In July 2020, the Court of Justice of the European Union (CJEU) ruled in *Schrems II* that the United States did not provide an adequate level of personal data protection.[7] The U.S.-EU divide over online data privacy, exacerbated in 2013 by Edward Snowden,[8] is now back to its starting point.[9] In December 2020, the EU publicized two major proposed legislations on the internet: the Digital Markets Act and the Digital Services Act.[10] The first regulates the behavior and policy of large digital platforms (the "gatekeepers") in creating contestable procedure and fair market conditions for small businesses; the second is focused on digital service providers and a new supervisory mechanism for creating a transparent and safe environment. These laws, considered by the *Wall Street Journal* to be the "most ambitious internet laws since the GDPR

---

[7] Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559 (July 16, 2020). This case followed Case C-362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650 (Oct. 6, 2015). Between the two cases, a major legal framework on privacy was updated in the EU. *See* Commission Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119). Following the CJEU's decision in *Schrems II,* the Irish Data Protection Commission commenced an inquiry to consider whether the actions of Facebook Ireland's transfer of personal data relating to individuals in the European Union was lawful, but that inquiry was challenged by Facebook Ireland in Irish High Court, leading to a judgment on May 14, 2021. Facebook Ir. Ltd. v. Data Prot. Comm'n [2021] IEHC 336 (Ir.). The issues raised by Facebook Ireland were procedural, but it looks like the dispute is far from over.

[8] *See generally* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (1st ed. 2014) (describing data privacy in the wake of Edward Snowden's revelations).

[9] *See generally* Paul M. Schwartz, *The EU-U.S. Privacy Collision A Turn to Institutions and Procedures,* 126 HARV. L. REV. 1966 (2013) [hereinafter Schwartz, *The EU-U.S. Privacy Collision*]; Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law,* 106 GEO. L.J. 115 (2017) [hereinafter Schwartz & Peifer]. *See also* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace,* 52 STAN. L. REV. 1315, 1318 (2000) (showing the difference between the EU and the U.S. in the early 2000s).

[10] *Commission Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act),* COM (2020) 842 final (Dec. 15, 2020); *Commission Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC,* COM (2020) 825 final (Dec. 15, 2020).

[General Data Protection Regulation],"[11] if passed as proposed, would significantly change the regulatory landscape.

Despite their fundamental differences, both the EU and China frame their cyber law and policy in terms of "sovereignty." In China, President Xi Jinping started talking about "cyber sovereignty" in 2015.[12] The term "cyber sovereignty," vague as it is, is used to justify political control of the internet and to create a protected space for domestic industry.[13] The EU also found the notion attractive but formulated it slightly differently, calling it "digital sovereignty." In a brief to the European Parliament in February 2020, digital sovereignty was defined as "Europe's ability to act independently in the digital world."[14] It seems clear what brought China and the EU together in asserting "sovereignty" in cyberspace is that they both feel the need to reclaim the power to control and regulate the internet.

In the United States, however, the same word "sovereignty" was used in the early 1990s by internet visionaries to mean the *opposite*—they have imagined a world free from government regulations, with the internet itself constituting a utopia characterized by self-governance.[15] Over the

---

[11] Sam Schechner, *Tech Giants Face New Rules in Europe, Backed by Huge Fines,* WALL ST. J. (Dec. 16, 2020, 7:48 AM), https://www.wsj.com/articles/tech-giants-face-new-rules-in-europe-backed-by-huge-fines-11608046500 [https://perma.cc/AA67-3MQX].

[12] *China Allows no Compromise on Cyberspace Sovereignty,* Renmin Ribao (人民日报) [PEOPLE'S DAILY] (Dec. 17, 2015, 7:20 AM). http://en.people.cn/n/2015/1217/c90000-8991532.html# [https://perma.cc/7E5N-PUCU] (last visited Sept. 25, 2021). Anqi Wang, *Cyber Sovereignty at its Boldest A Chinese Perspective,* 16 OHIO ST. TECH. L.J. 395, 397 (2020). *See generally* Wangluo Zhuquan: Lilun yu Shijian (网络主权：理论与实践)[Cyber Sovereignty: Theory and Practice] Oct. 21, 2019, https://2019.wicwuzhen.cn/web19/release/201910/t20191021_11229796.shtml [https://perma.cc/2Q6P-W3QW] (last visited May 30, 2021).

[13] ELIZABETH C. ECONOMY, THE THIRD REVOLUTION: XI JINPING AND THE NEW CHINESE STATE 55–90 (1st ed. 2018).

[14] Tambiama Madeiga (Eur. Parliamentary Rsch. Serv. Ideas Paper), *Digital Sovereignty for Europe*, at 1, PE 651.992 (July 2020). *See also* Jonathan Hackenbroich, *Reality Bytes Europe's Bid for Digital Sovereignty,* EUR. COUNCIL ON FOREIGN RELS. (Oct. 17, 2018), https://ecfr.eu/article/commentary_reality_bytes_europes_bid_for_digital_sovereignty/ [https://perma.cc/SV2Y-7YTH] (explaining the tools Europe has to influence and control the internet in an American- and Chinese-dominated digital world).

[15] *See generally* David R. Johnson & David Post, *Law and Borders–The Rise of Law in Cyberspace,* 48 STAN. L. REV. 1367 (1996) (discussing internet regulations during the 1990s); Henry H. Perritt, Jr., *Cyberspace Self-Government Town Hall Democracy or Rediscovered Royalism,* 12 BERKELEY TECH. L.J. 413 (1997) (advocating that self-governance of the Internet is desirable and legally feasible); Joanna Zakalik, *Law Without Borders in Cyberspace,* 43 WAYNE L. REV. 101 (1996) (arguing against internet regulations); Lawrence Lessig, *The Path of Cyberlaw,* 104 YALE L.J. 1743 (1995) (discussing the path to regulating the internet). *Compare* Henry H. Perritt, Jr., *The Internet as a Threat to Sovereignty–Thoughts on the Internet's Role in Strengthening National and*

years, this belief became weaker,[16] but the association of internet with freedom remained unshaken—in 2012, the Arab Spring was hailed as the "Facebook Revolution" in the United States.[17] It was not until the Facebook/Cambridge Analytica scandal, revealed in 2018,[18] that social media began to be perceived as a major threat to democracy because it allowed a foreign actor (Russia) to influence U.S. elections. In her recent book, *The Revolution That Wasn't*, sociologist Jen Schradie explains how conservative groups used social media more effectively in their political mobilization.[19] Shoshana Zuboff, a professor from the Harvard Business School, characterizes contemporary digital economy as "surveillance capitalism," where "every casual search, like, and click was claimed as an asset to be tracked, parsed, and monetized by some company. . . ."[20] This "new breed of economic power," according to Zuboff, forcefully seduces every trusting consumer into its powerful vortex: "the precise moment at

---

Global Governance, 5 IND. J. GLOB. LEGAL STUD. 423, 434 (1998) (explaining how the internet could engage in self-governance), *with* Saskia Sassen, *On the Internet and Sovereignty*, 5 IND. J. GLOB. LEGAL STUD. 545 (1998) (responding to other arguments on internet sovereignty). *But see* Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403 (1996); Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOB. LEGAL STUD. 475 (1998); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1119 (1998); Timothy S. Wu, *Cyberspace Sovereignty?—The Internet and the International System*, 10 HARV. J.L. & TECH. 647 (1997); JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET: ILLUSIONS OF A BORDERLESS WORLD (2006).

[16] Lawrence Lessig observed in 2006, "[i]n the years since [1999], that common view has faded. The confidence of the internet exceptionalists has waned. The idea—and even the desire—that the internet would remain unregulated is gone." LAWRENCE LESSIG, CODE VERSION 2.0, at ix (2d ed. 2006).

[17] *See* Jose Antonio Vargas, *Spring Awakening How an Egyptian Revolution Began on Facebook*, N.Y. TIMES (Feb. 17, 2012), https://www.nytimes.com/2012/02/19/books/review/how-an-egyptian-revolution-began-on-facebook.html [https://perma.cc/6R26-GZ84]; Anupam Chander, Essay, *Jasmine Revolutions*, 97 CORNELL L. REV. 1505 (2012). *But see* Marc Lynch, *After Egypt The Limits and Promise of Online Challenges to the Authoritarian Arab State*, 9 PERSP. ON POL. 301, 302 (2011) ("For all their dizzyingly effective use by creative young activists, it is not obvious that these new media exclusively challenge the competencies of authoritarian states.").

[18] Nicholas Confessore, *Cambridge Analytica and Facebook The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018) https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html [https://perma.cc/AH58-KG5N]. Two of the Cambridge Analytica whistleblowers, Chris Wylie and Brittany Kaiser, have published their memoirs on the events. *See* BRITTANY KAISER, TARGETED: THE CAMBRIDGE ANALYTICA WHISTLEBLOWER'S INSIDE STORY OF HOW BIG DATA, TRUMP, AND FACEBOOK BROKE DEMOCRACY AND HOW IT CAN HAPPEN AGAIN (1st ed. 2019); CHRISTOPHER WYLIE, MINDF*CK: CAMBRIDGE ANALYTICA AND THE PLOT TO BREAK AMERICA (1st ed. 2019).

[19] *See generally* JEN SCHRADIE, THE REVOLUTION THAT WASN'T: HOW DIGITAL ACTIVISM FAVORS CONSERVATIVES (2019) (arguing that conservative groups use social media more effectively in political mobilization).

[20] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN NATURE AT THE NEW FRONT OF POWER 52 (1st ed. 2019).

which our needs are met is also the precise moment at which our lives are plundered for behavioral data, and all for the sake of others' gain."[21] Zuboff warns, cyberspace is no different from the physical world: "[i]n our enthusiasm and growing dependency on technology, we tended to forget that the same forces of capital from which we had fled in the 'real' world were rapidly claiming ownership of the wider digital sphere."[22]

This significant shift in the perception of social media, and the internet in general, calls for a more engaging understanding of the regulatory concerns of global society and its regulatory division.[23] This Article aims to develop such a global perspective. It is based on a taxonomy of the digital world which is divided into three camps. The first camp is the United States as the global center of the internet—home to global digital platforms such as Microsoft, Google, Facebook, Amazon, and Twitter, etc. The global center has commercial, strategic, and ideological interests in keeping the internet an autonomous, self-contained system that enables a free flow of data on the global level. The second camp includes major data consumption countries—the Commonwealth countries (Great Britain, Canada, Australia, etc.), the European Union, and Japan. These are developed economies based on modern technology, before the internet era, who now lag behind after the "lost decades."[24] The open nature of their economies and their political alliances with the United States makes them ideal consumers in the digital economy. However,

---

[21] *Id.* at 52–53.

[22] *Id.* at 47.

[23] In the United States, the Biden Administration appointed a number of experts critical of Big Tech, suggesting that the administration will be more serious in enforcing antitrust laws in America. Cecilia Kang, *A Leading Critic of Big Tech Will Join the White House*, N.Y. TIMES (Mar. 5, 2021), https://www.nytimes.com/2021/03/05/technology/tim-wu-white-house.html [https://perma.cc/4722-ENJ6]; David McCabe & Cecilia Kang, *Biden Names Lina Khan, a Big-Tech Critic, as F.T.C. Chair*, N.Y. TIMES (June 15, 2021), https://www.nytimes.com/2021/06/15/technology/lina-khan-ftc.html [https://perma.cc/N3JM-HTPC]; Ryan Tracy & Aruna Viswanatha, *Biden to Nominate Jonathan Kanter as Chief of Justice Department's Antitrust Division*, WALL. ST. J. (July 20, 2021), https://www.wsj.com/articles/jonathan-kanter-to-be-nominated-as-doj-antitrust-chief-white-house-says-11626805273 [https://perma.cc/K2BX-6JKV].

[24] In Japan, it is widely believed that the "late digitalization" was the main reason behind Japan's stagnation. *See* Shōsansei, Nihon wa Ressei Tsudzuku – Dejitaru-ka Okure Eikyō Ka [*Productivity Continues to be Inferior in Japan Widening Gap with the Average of Developed Countries*], JAPANESE ECON. NEWS (Mar. 23, 2020), https://www.nikkei.com/article/DGKKZO57082100S0A320C2NN1000/ [https://perma.cc/SB55-YXJ8]. In 2019, the United Nations Conference on Trade and Development (UNCTAD), an agency of the United Nations, reported that measured by market capitalization of major digital platforms, Europe's share was only 4 percent. U.N. CONF. ON TRADE & DEV., DIGITAL ECONOMY REP. 2019, at xvi (2019).

these countries are concerned about losing their competitive edge in the digital economy or even control in modern social life;[25] they tend to treat the internet as a global institution with suspicion. Their liberal democracies give them strong instincts and their sophisticated legal frameworks provide tools to regulate the behavior of the global digital platforms, most of which are based in Silicon Valley. This second camp tends to adopt legal rules from the perspective of the consumer.

The third camp is China, which considers itself an ideological and technological rival to the United States. Its initial efforts to split the internet—when it kicked Google out of the Chinese market and built the "Great Firewall" (China's online censorship system)—were to defend and preserve its political regime.[26] Today, China's e-commerce market is worth $2 trillion, more than America's and Europe's combined.[27] Tencent, Alibaba, and Baidu became major digital platforms, and Huawei and ZTE became major manufacturers in China's digital economy.[28] Like the second camp, China has its own concerns. On the one hand, the regime is heavily dependent on the tech firms for its global strategy and ambition, as well as for their capacity and data for domestic control.[29] On the other hand, however, these tech firms are all "private" enterprises and thus must

---

[25] *See* Valentina Romei, *EU Faces Long Road Ahead as it Tries to Catch Digital Leaders in US and China*, FIN. TIMES, Dec. 17, 2019, at 3. In Japan, for example, *Nippon Keizai Shimbun*, a major national newspaper, warned of the ongoing revolution of global economy based on "invisible assets." Miezaru Shisan, Seichō No Minamoto Ni [Invisible Assets Become Source of Growth], Nihonkeizaishinbun [JAPANESE ECON. NEWS] (Feb. 25, 2019), https://www.nikkei.com/article/DGXMZO41629950S9A220C1SHA000/ [https://perma.cc/K9PQ-WG64]. For a broad analysis of Japan's tech sectors, *see generally* MARIE ANCHORDOGUY, REPROGRAMMING JAPAN: THE HIGH TECH CRISIS UNDER COMMUNITARIAN CAPITALISM (Peter J. Katzenstein, ed., Cornell Univ. Press 2005).

[26] ECONOMY, *supra* note 13; *See generally* JAMES GRIFFITHS, THE GREAT FIREWALL OF CHINA: HOW TO BUILD AND CONTROL AN ALTERNATIVE VERSION OF THE INTERNET (1st ed. 2019); Haiping Zheng, *Regulating the Internet China's Law and Practice*, 4 BEIJING L. REV. 37 (2013). Prior to the Golden Shield Program, online activism was already posing a challenge to the Chinese Regime. *See* GUOBIN YANG, THE POWER OF THE INTERNET IN CHINA: CITIZEN ACTIVISM ONLINE (1st ed. 2009).

[27] *The Future of Global E-Commerce,* THE ECONOMIST., Jan. 2, 2021, at 10.

[28] UNCTAD noted that "[t]he economic geography of the digital economy does not display a traditional North-South divide. It is consistently being led by one developed and one developing country: the United States and China." U.N. Conf. on Trade & Dev., *supra* note 24, at xvi. *See generally* Ludwig Siegele, *Special Report The Data Economy*, THE ECONOMIST. (Feb. 20, 2020), https://www.economist.com/special-report/2020-02-22 [https://perma.cc/3K9R-GDE7].

[29] *See* Jing Yang, *Beijing Tracks Dissent over Ubiquitous App*, WALL ST. J., Dec. 23, 2020, at A8.

be brought under control by the Party State.[30] For this reason, China also treats the internet with suspicion and uses policy to regulate it.

This Article argues that the second and third camps not only share a common interest in reclaiming sovereignty in cyberspace based on their *regulatory* needs, but also, in the recent past, have aggressively adopted similar regulatory policies in filling the vacuum in cyberspace. Together, they took different legal positions from the U.S. and developed their own legal rules: their courts increasingly claim rather than decline jurisdiction over nonresident digital platforms; they have all adopted tort standards in deciding liability rather than offering a broad immunity; and furthermore, their courts are more open to using global injunction orders as remedy against digital platforms who are innocent non-parties in disputes. All of these actions by the second and third camps have resulted in what I have termed a revolt against the U.S. hegemony in cyberspace.

This Article contributes to our understanding of the current state of cyber law. The global perspective demonstrates an almost uniform response to the U.S. law in cyberspace from all of America's major trading partners. In the past, comparative studies tended to focus on a single jurisdiction—typically, the European Union—and compared it with the United States. This approach, informative as it was, significantly understated the gravity of the differences between that jurisdiction and the United States. Fundamentally, it was based on an American-centric outlook with primary interests in building convergence models.[31] In cyberspace, however, this is simply not helpful.[32] In recent years, scholars

---

[30] Lingling Wei, *To Curb Ma's Empire, China Weighs Taking a Bigger Stake*, WALL ST. J., Dec. 30, 2020, at A1. On the founding of Alibaba, *see generally* DUNCAN CLARK, ALIBABA: THE HOUSE THAT JACK MA BUILT (1st ed. 2016). However, since 2017, the Chinese government has started trying to control big tech in China. *See* Raymond Zhong & Sui-Lee Wee, *China Seeks Small Stakes in Online Companies, and More Power Over Them*, N.Y. TIMES, Oct. 14, 2017, at B3. *See generally* Curtis J. Milhaupt & Wentong Zheng, *Beyond Ownership State Capitalism and the Chinese Firm*, 103 GEO. L.J. 665 (2015) (discussing the control of private firms in China).

[31] *See generally* Anne-Marie Slaughter, *A Global Community of Courts*, 44 HARV. INT'L L.J. 191 (2003) (discussing global shifts in transnational litigation); Anne-Marie Slaughter, *Judicial Globalization*, 40 VA. J. INT'L L. 1103 (2000) (examining constitutional cross-fertilization); ANNE-MARIE SLAUGHTER, A NEW WORLD ORDER (1st ed. 2004).

[32] Anne-Marie Slaughter's network theory was initially followed by Paul M. Schwartz in his earlier analysis of EU-US efforts on privacy before the GDPR. *See* Schwartz, *The EU-U.C. Privacy Collision*, *supra* note 9, at 1967. However, Professor Schwartz's narrative for post-GDPR EU-U.S. relationship has shifted. *See* Schwartz & Peifer, *supra* note 9 (contrasting the "rights talk" at EU and the "marketplace discourse" in the United States). *See generally* Paul M. Schwartz, *Global Data Privacy The EU Way*, 94 N.Y.U. L. REV. 771 (2019) (examining the regulatory environment of international data protection) [hereinafter Schwartz, *Global Data Privacy*].

of the European Union have argued for the "Brussels effect,"[33] which contended that EU's more strict regulatory approach in cyberspace not only persists but is now followed by many countries outside Europe. The global perspective adopted in this Article follows the direction of the regulatory theories and pushes the logic to its end. By examining cases from five jurisdictions, this Article demonstrates not only that there is divergence in cyberspace regulation but that the United States is a lone outlier in its regulatory approach to the internet, while the other four jurisdictions—the European Union, the Commonwealth countries, Japan, and China—have all adopted a more rigorous regulatory approach. It is a revolt.

In the remainder of this Article, Part I lays the foundation for the comparison by describing the legal frameworks in the United States. It tracks the development of legal doctrines in two critical areas. First, this Article examines personal jurisdiction over nonresident defendants in defamation and intellectual property cases. Second, it analyzes the jurisprudence of Section 230 of Communications Decency Act (CDA),[34] which provides immunity to digital platforms. Part II then provides a comparison of personal jurisdiction issues in laws and judicial cases in four jurisdictions: the Commonwealth countries, the European Union, Japan, and China. In contrast with the more limited personal jurisdiction doctrines in the United States, the other four jurisdictions made it easier for victims to establish personal jurisdiction and thus have access to courts. Part III tracks legal doctrines on liability of digital platforms in the four jurisdictions. In contrast with the general immunity in the United States under Section 230 of the CDA, all four jurisdictions adopted tort liability for digital platforms. Part IV tracks legal doctrines in global injunctions by courts in the four jurisdictions to show a general move toward more willingness to extend remedy beyond their borders. The global revolt in cyberspace described in this Article is a significant development in the twenty-first century, with critical policy ramifications. Some final thoughts will be discussed in the conclusion.

---

[33] Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 3 (2012) (discussing Europe's "unilateral power to regulate global markets" as tending to penetrate and influence other countries to adopt similar measures). *See also* Schwartz, *Global Data Privacy*, *supra* note 32, at 771 (noticing EU's GDPR is widely regarded as a privacy law not just for the EU but for the world).

[34] 47 U.S.C. § 230.

I. CYBERSPACE ACCORDING TO U.S. LAW

As the birthplace of the internet and home to global digital platforms such as Microsoft, Apple, Google, Facebook, and Amazon, the United States potentially has a central role in regulating the internet. However, the American regulations are built on a strikingly counterintuitive principle: self-regulation. This is reflected in two areas of law regulating cyberspace. The first area is personal jurisdiction, which is procedural law that determines whether the digital platforms are within the reach of courts. In cyberspace, power is highly concentrated in a small number of digital platforms that are not in the same jurisdiction as the vast majority of the hundreds of millions of users around the world. They are typically not the perpetrator who wrote the defamatory statement or posted the video in violation of copyright law. In other words, they are non-resident, third-party defendants.

In the United States, in order to assert personal jurisdiction, a plaintiff is required to establish "minimum contacts" under the Due Process Clause of the Fourteenth Amendment and state law.[35] While the United States Supreme Court has not spoken on the issue since the arrival of the internet,[36] lower federal courts and state courts often require a more demanding "minimum contacts," making the court less accessible. The second area of law is Section 230 of the CDA,[37] a federal statute granting general immunity to digital platforms and service providers from civil liability. As will be discussed in detail, federal courts largely follow a "bright-line rule" approach in interpreting Section 230 as a broad

---

[35] *See infra* text accompanying notes 39–41.

[36] *See generally* Patrick J. Borchers, *Internet Libel The Consequences of a Non-Rule Approach to Personal Jurisdiction*, 98 NW. U. L. REV. 473 (2004) (analyzing jurisdiction questions in a series of internet-related cases). This is at odds with repeated reflections of the Supreme Court that jurisdictional issues were driven by the commercial and technological transformation of the American economy. In 1979, Justice White noted that "[t]he limits imposed on state jurisdiction by the Due Process Clause, in its role as a guarantor against inconvenient litigation, have been substantially relaxed over the years . . . this trend is largely attributable to a fundamental transformation in the American economy." World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 293 (1980). Similarly, Justice Black once commented, "[l]ooking back over this long history of litigation a trend is clearly discernible toward expanding the permissible scope of state jurisdiction over foreign corporations and other nonresidents. In part this is attributable to the fundamental transformation of our national economy over the years." McGee v. Int'l Life Ins. Co., 355 U.S. 220, 222 (1957).

[37] 47 U.S.C. § 230.

immunity based on the distinction between "publisher" and "distributor."[38] These two areas serve a common goal: self-regulation.

A. CONSTITUTIONAL FRAMEWORK FOR JURISDICTION

Before the arrival of the internet, personal jurisdiction over a nonresident defendant had moved from strict territoriality to a more flexible "minimum contacts" theory under the Due Process Clause.[39] In the seminal decision *International Shoe Co. v. Washington*, the United States Supreme Court declared that "in order to subject a defendant to a judgment *in personam*, if he be not present within the territory of the forum, he must have certain minimum contacts with it such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'"[40] The question, however, is how to define "minimum contacts."[41] On March 20, 1984, the United States Supreme Court delivered opinions for two libel cases, both written by Justice Rehnquist. So far, these are the ultimate guide for U.S. tort cases in the internet age.

---

[38] *See* discussion *infra* text accompanying notes 88–91.

[39] Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945), *overruling* Pennoyer v. Neff, 95 U.S. 714 (1878). The United States Supreme Court later ruled that state courts must follow *International Shoe* standards when asserting in rem jurisdiction as well, thus concluding the transition from territoriality in *Pennoyer* to the "minimum contacts" standards in *International Shoe*. *See* Shaffer v. Heitner, 433 U.S. 186 (1977). *See also* Linda J. Silberman, Shaffer v. Heitner: *The End of an Era*, 53 N.Y.U. L. REV. 33, 34–35 (1978).

[40] *Int'l Shoe Co.*, 326 U.S. at 316 (citation omitted).

[41] Many commentators have argued the United States Supreme Court has not clarified the issue in a string of cases. *See* Hanson v. Denckla, 357 U.S. 235, 253 (1958); World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980) ("When a corporation 'purposefully avails itself of the privilege of conducting activities within the forum state' . . . it has clear notice that it is subject to suit there. . . ."); Burger King Corp. v. Rudzewicz, 471 U.S. 462, 472 (1985) ("Where a forum seeks to assert specific jurisdiction over an out-of-state defendant who has not consented to suit there, this 'fair warning' requirement is satisfied if the defendant has 'purposefully directed' his activities at residents of the forum . . ."); Asahi Metal Indus. Co., Ltd. v. Super. Ct. of Cal., 480 U.S. 102, 112 (1987) ("The 'substantial connection,' between the defendant and the forum State necessary for a finding of minimum contacts must come about by an action of the defendant purposefully directed toward the forum State. The placement of a product into the stream of commerce, without more, is not an act of the defendant purposefully directed toward the forum State."); J. McIntyre Machinery, Ltd. v. Nicastro, 564 U.S. 873, 886–87 (2011). *See generally* Henry S. Noyes, *The Persistent Problem of Purposeful Availment*, 45 CONN. L. REV. 41 (2012) (discussing the recurring question of defining purposeful availment and proposing a definition). In *Bristol-Myers Squibb v. Super. Ct. of Cal.*, 137 S. Ct. 1773, 1786 (2017), the question of purposeful availment was not in dispute, but the court analyzed jurisdiction at length.

1. Keeton *and* Calder

The Court developed the doctrine called "purposeful availment" in the case *Keeton v. Hustler Magazine*.[42] Here, a resident of New York brought a libel suit in New Hampshire state court against an Ohio publisher whose principal place of business was in California. On minimum contacts, the Court stated that

> the contacts between respondent and New Hampshire must be such that it is "fair" to compel respondent to defend a multistate lawsuit in New Hampshire seeking nationwide damages for all copies of the five issues in question, even though only a small portion of those copies were distributed in New Hampshire.[43]

The Court found the publisher's regular circulation of its magazines sufficient to support personal jurisdiction: "Where, as in this case, respondent *Hustler Magazine, Inc.*, has continuously and deliberately exploited the New Hampshire market, it must reasonably anticipate being hauled into court there in a libel action based on the contents of its magazine."[44]

In *Calder v. Jones*,[45] however, a unanimous Court adapted the purposeful availment doctrine to intentional tort cases. Here, the plaintiff was a California resident, filing a complaint in California state court against the *National Enquirer*, a national magazine with its principal place of business in Florida. The other two defendants—the author and editor of the defamatory article—were both Florida residents. In judging minimum contacts, the Court reasoned, a court should focus on "the relationship among the defendant, the forum, and the litigation."[46] The unanimous Court adopted an "effect" theory: "[h]ere, the plaintiff is the *focus* of the activities of the defendants out of which the suit arises."[47] The Court highlighted the following facts of the case:

---

[42] Keeton v. Hustler Mag., Inc., 465 U.S. 770, 774–802 (1984).

[43] *Id.* at 775.

[44] *Id.* at 781.

[45] Calder v. Jones, 465 U.S. 783, 788–791 (1984).

[46] *Id.* at 788. *Id.* In *Shaffer v. Heitner*, 433 U.S. 186, 204 (1977), when tracking the history of *International Shoe* jurisprudence, Justice Marshall wrote: "the relationship among the defendant, the forum, and the litigation, rather than the mutually exclusive sovereignty of the States on which the rules of *Pennoyer* rest, became the central concern of the inquiry into personal jurisdiction."

[47] *Calder v. Jones*, 465 U.S. at 788 (emphasis added).

> [t]he allegedly libelous story concerned the California activities of a California resident. It impugned the professionalism of an entertainer whose television career was centered in California. The article was drawn from California sources, and the brunt of the harm, in terms both of respondent's emotional distress and the injury to her professional reputation, was suffered in California.[48]

Based on these facts, the Court concluded: "In sum, California is the *focal point* both of the story and of the harm suffered. Jurisdiction over petitioners is therefore proper in California based on the '*effects*' of their Florida conduct in California."[49]

So far, from the wording of the above statement, "effect" theory seemed sufficient for finding "minimum contacts." However, in response to petitioners' arguments, the *Calder* Court added a "targeting" element in order to distinguish intentional torts from product liability cases based on negligence. Here, the Court highlighted the following facts:

> Their intentional, and allegedly tortious, actions were *expressly aimed* at California. Petitioner South wrote and petitioner Calder edited an article that they knew would have a potentially devastating impact upon respondent. And they knew that the brunt of that injury would be felt by respondent in the State in which she lives and works and in which the *National Enquirer* has its largest circulation. Under the circumstances, petitioners must 'reasonably anticipate being hauled into court there' to answer for the truth of the statements made in their article.[50]

The Court therefore ruled that jurisdiction in California was proper because defendants' "intentional conduct in Florida calculated to cause injury to respondent in California."[51]

The "targeting" element in *Calder* appears to be a "purposeful direction" rule for intentional torts, similar to the "purposeful availment" doctrine for negligence.[52] If this is the case, then, *Calder* provides two theories of "minimum contacts"—effects and purposeful direction. While the factual pattern of *Calder* is a coherent combination of the two, *Keeton* is not. The forum state in *Keeton* was New Hampshire, whose only contact

---

[48] *Id.* at 788–89.

[49] *Id.* at 789 (emphasis added).

[50] *Id.* at 789–90 (emphasis added).

[51] *Id.* at 791.

[52] In *Burger King*, the Supreme Court treated this as the same rule. Burger King Corp. v. Rudzewicz, 471 U.S. 462 (1985). Later, the Supreme Court made it clear that "[its] 'minimum contacts' analysis looks to the defendant's contacts with the forum State itself, not the defendant's contacts with persons who reside there." Walden v. Fiore, 571 U.S. 277, 285 (2014).

with the magazine in question was the latter's circulation. There was no additional "targeting."

The Supreme Court has not ruled on personal jurisdiction in defamation cases since the advent of the internet age.[53] Federal courts and state courts have struggled with the ambiguity of *Calder* and *Keeton* and translating the purposeful availment doctrine into rules for the online world. They can be divided into two schools of thought: a minority of the state courts adopt *Calder* into an "effect" theory; other courts are not satisfied with "effect" alone, and require a "targeting" element. The latter approach makes it harder for internet users to establish personal jurisdiction over a nonresident thirty-party digital platform.

2. The "Effect" Theory

Among state courts, Ohio and Florida find *Calder* directly applicable in online defamation cases. In *Kauffman Racing Equipment v. Roberts*,[54] a decision by the Supreme Court of Ohio, a seller of automobile engine blocks based in Ohio filed a libel complaint in state court against Scott Roberts, a customer based in Virginia, for the latter's online postings on various websites devoted to automobile racing equipment. A majority of the Ohio Supreme Court concluded that personal jurisdiction was justified because the tort occurred in Ohio, even though online:

> Roberts posted his allegedly defamatory statements on the Internet, ostensibly for the entire world to see. How much of the world saw the comments is unknown; but we do know that at least five Ohioans saw Roberts's statements. The comments were thus published in Ohio. Because Roberts's allegedly defamatory statements were published in Ohio, his alleged tort was committed in Ohio, and he falls within the grasp of [Ohio's long-arm statute].[55]

The Ohio Supreme Court noted that *Calder* itself did not involve internet communication, but considered the factual pattern in *Calder* similar enough.[56] As in *Calder*, the majority of the Ohio Supreme Court concluded that "[t]he effects analysis necessitates conduct 'calculated to cause injury' in a 'focal point' where the 'brunt' of the injury is experienced."[57]

---

[53] Borchers, *supra* note 36, at 475.

[54] Kauffman Racing Equip., L.L.C., v. Roberts, 930 N.E.2d 784, 789 (Ohio 2010).

[55] *Id.* at 791.

[56] *Id.* at 795.

[57] *Id.* at 796.

A similar question was raised in an Eleventh Circuit case, which certified that question to the Supreme Court of Florida.[58] There, the plaintiff was a recruiting firm based in Nevada with its principal place of business in Florida; defendant was a resident of Washington State who owned and operated a non-commercial website on consumer-related issues. The Supreme Court of Florida concluded that "allegedly defamatory material about a Florida resident placed on the Web and accessible in Florida constitutes an 'electronic communication into Florida' when the material is accessed (or 'published') in Florida."[59] What is in common between the Florida and Ohio Supreme Courts is that they took *Calder*'s effect theory as sufficient ground for asserting jurisdiction; they did not ask for the targeting element. In the online world, the effect-only standard makes the court easily accessible to plaintiffs. However, other states and federal courts are not comfortable with this approach. Rather, they demand both elements in *Calder*—effect plus targeting—in order to meet the Due Process requirement.

3. The "Effect Plus Targeting" Theory

In *Griffis v. Luban*, the Minnesota Supreme Court ruled that a court in Alabama did not have personal jurisdiction over a resident in Minnesota for critical postings on an online newsgroup.[60] In discussing the jurisprudence, the Minnesota Supreme Court noted that the majority of "courts have consistently refused to find jurisdiction based on *Calder* merely because the plaintiff was located in the forum state and therefore felt the effects of the alleged intentional tortious conduct there."[61] "Instead," the court highlighted, "the courts have construed *Calder* as

---

[58] Internet Sols. Corp. v. Marshall, 557 F.3d 1293, 1296–97 (11th Cir. 2009) (certifying the legal question to the Supreme Court of Florida).

[59] Internet Sols. Corp. v. Marshall, 39 So. 3d 1201, 1214 (Fla. 2010). The Supreme Court of Florida distinguished defamatory material "accessible" and "accessed" in Florida:

> We conclude that posting defamatory material on a website alone does not constitute the commission of a tortious act within Florida. . . . Rather, the material posted on the website about a Florida resident must not only be *accessible* in Florida, but also be *accessed* in Florida in order to constitute the commission of the tortious act of defamation within Florida under [Florida statute].

Id. at 1203. The *Internet Solutions* ruling was later applied by the Eleventh Circuit. *See* Catalyst Pharms., Inc. v. Fullerton, 748 Fed. Appx. 944 (11th Cir. 2018).

[60] Griffis v. Luban, 646 N.W.2d 527, 536 (Minn. 2002).

[61] *Id.* at 533.

requiring more than mere effects in the forum state."[62] In California, the supreme court has not ruled on an online defamation case; but it ruled in a trade secret case that exercising personal jurisdiction solely based on internet postings violated Due Process.[63] The Court of Appeals for the Fourth District ruled in *Burdick v. Superior Court* that the posting of defamatory statements on Facebook itself was insufficient to create the minimum contacts necessary to support personal jurisdiction in a lawsuit against a non-resident.[64] More recently, the same court of appeals ruled in a defamation case against a resident in Canada; when the social media postings explicitly target California, it satisfies the minimum contacts requirement.[65]

In New York, the statutory language explicitly exempts causes of action for defamation.[66] New York courts recognize a "clear distinction between a situation where the only act which occurred in New York was the mere utterance of the libelous material and on the other hand, a situation where purposeful business transactions have taken place in New York giving rise to the cause of action."[67] The New York Court of Appeals answered this question in the *SPCA* case.[68] There, a New York animal shelter filed a defamation case against a donor, a non-profit corporation based in Ohio, who posted critical comments on its own website alleging mistreatment of animals at the shelter.[69] The question became whether the defendants' activities—two short visits and three telephone conversations with the shelter, plus a donation of cash—constituted "purposeful activities" related to the alleged defamation.[70] The court of appeals concluded that they did not.[71] Not only did the court consider that these activities were "quite limited,"[72] but also said, "there is no substantial relationship between the allegedly defamatory statements and defendants' New York activities."[73]

---

[62] *Id.*

[63] Pavlovich v. Superior Court, 58 P.3d 2, 10–11 (Cal. 2002).

[64] Burdick v. Superior Court, Cal. Rptr. 3d 1, 12 (Ct. App. 2015).

[65] San Pedro v. Menorca, No. G058050, 2020 Cal. App. Unpub. LEXIS 4852 at *15–16 (July 29, 2020).

[66] N.Y. C.P.L.R. § 302(a) (McKinney 2020).

[67] Legros v. Irving, 327 N.Y.S.2d 371, 373 (App. Div. 1971).

[68] SPCA of Upstate N.Y. Inc. v. Am. Working Collie Ass'n, 963 N.E.2d 1226, 1228–30 (N.Y. 2012).

[69] *Id.* at 1228.

[70] *Id.* at 1228–29.

[71] *Id.* at 1229.

[72] *Id.*

[73] *Id.*

The Second Circuit shared the same view. In *Best Van Lines*,[74] a moving company based in New York filed a suit in federal court in New York against Tim Walker, a resident of Iowa who owned and operated a website giving information and reviews of house movers. Applying New York law, the Second Circuit concluded that "the nature of Walker's comments does not suggest that they were purposefully directed to New Yorkers rather than a nationwide audience." [75] In coming to this conclusion, the Second Circuit follows the jurisprudence that "New York courts construe 'transacts any business within the state' more narrowly in defamation cases than they do in the context of other sorts of litigation."[76]

The Fourth Circuit did the same in *Young v. New Haven Advocate*, an online defamation case.[77] Similarly, in *Revell v. Lidov*, the Fifth Circuit did not find a university website containing an allegedly defamatory article constituted substantial contacts under the Texas long-arm statute.[78] The Seventh Circuit is shifting its position from its earlier broad application of *Calder* to a position that is more open to inquire for "something more," as can be seen in *Tamburo v. Dworkin*.[79] The First Circuit has not spoken on this issue. The District Court for the District of Massachusetts has ruled in favor of a restrictive reading of *Calder* and adopted the *Zippo* test.[80] Similarly, the Ninth Circuit has not spoken on the issue.[81] In trademark

---

[74] Best Van Lines, Inc. v. Walker, 490 F.3d 239, 240 (2d Cir. 2007).

[75] *Id.* at 248.

[76] *Id.* at 253.

[77] *See* Young v. New Haven Advocate, 315 F.3d 256 (4th Cir. 2002) (construing Virginia's long-arm statute). *See also* ALC Scan, Inc. v. Digit. Serv. Consultants, Inc., 293 F.3d 707 (4th Cir. 2002) (construing Maryland's long-arm statute).

[78] Revell v. Lidov, 317 F.3d 467, 473–76 (5th Cir. 2002).

[79] Tamburo v. Dworkin, 601 F.3d 693, 706 (7th Cir. 2010) (Illinois long-arm statute). The Seventh Circuit emphasized in its conclusion:

> although they acted from points outside the forum state, these defendants specifically aimed their tortious conduct at [plaintiff] and his business in Illinois with the knowledge that he lived, worked, and would suffer the 'brunt of the injury' there. These allegations suffice to establish personal jurisdiction over these defendants under either a broad or a more restrictive view of *Calder*.

Id. at 706.

[80] *See* Broadvoice Inc. v. TP Innovations, L.L.C., 733 F. Supp. 2d 219, 226 (D. Mass. 2010) (construing Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997)).

[81] In an unpublished opinion, *Healthcare Alliance Inc. v. Healthgrades.com, Inc.*, 50 Fed. App'x 339 (9th Cir. 2002), the Ninth Circuit leaned towards a direct application of *Calder*. In this case, the defendant was a Delaware corporation with its principal place of business in Colorado that operated a website that rated home health care providers. *Id.* at 339. Plaintiff, a Washington State-based home health care provider, filed a suit after learning it had received what it considered an unfavorable rating on defendant's website. *Id.* at 339–40. The district court dismissed the case for

and copyright cases, the Ninth Circuit demanded "more" than what *Calder* requires.[82] One federal district court in the Ninth Circuit believes that "the Ninth Circuit as well as the majority of jurisdictions, have rejected the holding that merely posting information on an otherwise passive website is sufficient."[83]

In cyberspace, the majority of the federal and state courts in the United States require a "targeting" element in their interpretation of the "purposeful availment" doctrine in *Calder*. By contrast, as will be discussed in Part II, not all other jurisdictions required this targeting element. Requiring "targeting" makes the court much less accessible for internet users.

B. SECTION 230 OF THE CDA

The second area of law is a general immunity granted to digital platforms and internet service providers under Section 230, which was initially enacted in 1996 as part of Title V of the Telecommunications Act.[84] In June 1997, however, the United States Supreme Court struck down part of it for abridging freedom of speech protected by the First

---

lack of personal jurisdiction as it found defendant's website merely a passive provider of information. *Id.* at 340. The Ninth Circuit, relying on *Calder*, found that the defendant "has purposefully interjected itself into the Washington state home-healthcare market through its intentional act of offering ratings of Washington medical service providers. This act was expressly aimed at plaintiff's forum state. . . ." *Id.* at 341. *But see* 9TH CIR. R. 36-3(a) (circuit rule establishing that unpublished dispositions of the court are not precedent); Pedroza v. BRB, 624 F.3d 926, 931 (9th Cir. 2010) ("[A]n unpublished decision is not precedent for our panel.").

[82] In a trademark case, for example, *see* Bancroft & Masters, Inc. v. Augusta National Inc., 223 F.3d 1082, 1087 (9th Cir. 2000), *overruled on other grounds by* Yahoo! Inc. v. La Ligue Contre Le Racisme, 433 F.3d 1199 (9th Cir. 2006) (en banc) ("We have said [in *Panavision*] that there must be 'something more,' but have not spelled out what that something more must be. . . . We now conclude that 'something more' is what the Supreme Court described as 'express aiming' at the forum state."). For a copyright case, see *Mavrix Photo, Inc.*, in which the Ninth Circuit interpreted *Calder* as requiring express aiming to establish jurisdiction. Mavrix Photo, Inc. v. Brand Techs., Inc., 647 F.3d 1218, 1229 (9th Cir. 2011).

[83] Medihah Mining, Inc. v. Amunategui, 237 F. Supp. 2d 1132, 1135 (D. Nev. 2002). The court noted here that there was no evidence that any Nevada resident actually did access the alleged defamation. *Id.* at 1136. The court concluded that plaintiff failed to allege defamatory postings were directed at forum state. The District Court for the Western District of Washington agreed with this position. *See* Phillips v. World Publishing Co., 822 F. Supp. 2d 1114, 1123–24 (W.D. Wash. 2011) ("[C]ourts should not focus too narrowly on the test's third prong—the effects prong—because 'something more' is needed in addition to a mere foreseeable effect. That 'something more' is 'express aiming.'") (quoting *Bancroft*, 223 F.3d at 1087).

[84] Telecommunications Act of 1996, Pub. L. 104-104, § 230, 110 Stat. 56, 137–39.

Amendment.[85] Section 230 became 230(c)(1): "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[86]

When the CDA was proposed in 1995, Senator James Exon (D-Neb.) was primarily driven by concerns of online pornography.[87] Its basic framework was based on the conceptual distinction between publisher and distributor in *Cubby, Inc. v. CompuServe Inc.*,[88] and its primary target was "content providers." [89] During congressional deliberations, *Stratton Oakmont, Inc. v. Prodigy Services Co.*, an internet tort case questioning the publisher-distributer distinction in *Cubby*,[90] caught the attention of lawmakers. Senator Coats specifically mentioned *Stratton Oakmont* during the Senate floor debate:

> I understand that in a recent N.Y. State decision, *Stratton Oakmont versus Prodigy*, the court held that an online provider who screened for obscenities was exerting editorial content control. This led the court to treat the online provider as a publisher, not simply a distributor, and to therefore hold the provider responsible for defamatory statements made by others on the system. I want to be sure that the intent of the amendment is not to hold a company who tries to prevent obscene or indecent material under this section from being held liable as a

---

[85] Reno v. ACLU, 521 U.S. 844, 849 (1997). *See also* Claudia Oliveri, *Congress Wrestles with the Internet*: ACLU v. Reno *and the Communications Decency Act*, 6 MEDIA L. & POL'Y 12 (1997). *See generally* Charles Nesson & David Marglin, *The Day the Internet Met the First Amendment Time and the Communications Decency Act*, 10 HARV. J.L. & TECH. 113 (1996) (discussing the constitutional challenges to the CDA leading to *Reno v. ACLU*).

[86] 47 U.S.C. § 230(c)(1).

[87] Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act Regulating Barbarians on the Information Superhighway*, 49 FED. COMMC'NS L.J. 51, 53 (1996). Vikas Arora, Note, *The Communications Decency Act Congressional Repudiation of the "Right Stuff,"* 34 HARV. J. ON LEGIS. 473, 474 (1997). *Regulating the Internet Should Pornography Get a Free Ride on the Information Superhighway - A Panel Discussion*, 14 CARDOZO ARTS & ENT. L.J. 343, 344–45 (1996).

[88] *See* Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 140–41 (S.D.N.Y. 1991) (holding that passive providers of online services and content were not charged with knowledge of, or responsibility for, the content on their network).

[89] H.R. REP. NO.104-458, at 190 (1996) (Conf. Rep.) ("This provision is designed to target the criminal penalties of new sections 223(a) and (d) at content providers who violate this section and persons who conspire with such content providers, rather than entities that simply offer general access to the Internet and other online content. The conferees intend that this defense be construed broadly to avoid impairing the growth of online communications through a regime of vicarious liability."). *See also* 47 U.S.C. § 230(e) (defining "information content provider" to mean "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.").

[90] Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. 1995).

> publisher for defamatory statements for which they would not otherwise have been liable.[91]

Section 230 became the fundamental U.S. policy for the internet era. In 2010, the United States Congress extended it beyond U.S. territory by instructing federal courts not to recognize or enforce foreign defamation judgments that are inconsistent with Section 230.[92] While it has faced challenges in recent years,[93] Section 230 still remains the law in the United States.[94] Over time, federal courts accumulated a number of cases on Section 230 showing that they tend to give generous immunity to digital platforms or internet service providers. This jurisprudence is reflected in three aspects: courts tend to read Section 230 broadly, thus brushing aside the role played by digital platforms; courts developed the notion of "material contribution" to measure the role of digital platforms when they cannot avoid the question; even notification is often not considered as a decisive factor in deciding negligence.

1. Broad Reading of Section 230

In early cases, courts adopted a broad reading of Section 230. The Fourth Circuit Court led the way through its decision in *Zeran v. America Online, Inc.*[95] Here, plaintiff Kenneth Zeran alleged defamatory messages posted on an America Online bulletin board by an unidentified person.

---

[91] 141 Cong. Rec. 16,024–25 (1995).

[92] 28 U.S.C. § 4102(c)(1); Securing the Protection of Our Enduring and Established Constitutional Heritage Act of 2010 § 4102, 28 U.S.C. § 4102.

[93] For example, see Exec. Order No. 13,925, 85 Fed. Reg. 34,079 (June 2, 2020), in which President Donald Trump used the executive order to attack Section 230. William Barr, U.S. Att'y Gen., Remarks at the National Association of Attorneys General 2019 Capital Forum (Dec. 10, 2019), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-national-association-attorneys-general [https://perma.cc/8HR4-BC8W]. On June 17, 2020, DOJ issued recommendations for Section 230 reform. *See* Press Release, U.S. Dep't of Just., Justice Department Issues Recommendations for Section 230 Reform (June 17, 2020), https://www.justice.gov/opa/pr/justice-department-issues-recommendations-section-230-reform [https://perma.cc/CV4W-GU2C]. The National Association of Attorneys General (NAAG) once endorsed an amendment to the Communications Decency Act of 1996. On July 24, 2013, forty-seven state attorneys general wrote a letter to Congressional leaders, asking Congress to amend Section 230 of the Communications Decency Act to carve all state criminal laws from the statute's protection. *See NAAG Supports Amendment to the Communications Decency Act* (May 23, 2019) https://www.naag.org/naag/media/naag-news/naag-supports-amendment-to-the-communications-decency-act.php [https://perma.cc/5TA4-K2KZ].

[94] *See generally* PAUL M. BARRETT, N.Y.U. STERN CENTER FOR BUSINESS AND HUMAN RIGHTS, REGULATING SOCIAL MEDIA: THE FIGHT OVER SECTION 230—AND BEYOND (2020) (discussing the controversy over the law and making recommendations for its improvement).

[95] Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).

Zeran notified America Online (AOL) of the messages but AOL did not take them down.[96] Zeran did not bring any action against the unidentified person who posted the offensive messages, but instead filed a complaint against AOL.[97] When AOL moved to dismiss the case based on CDA Section 230, the district court granted the motion.[98] Zeran appealed to the Fourth Circuit.[99]

In affirming the district court's decision, the Fourth Circuit framed Section 230 in terms much broader than was required for the fact pattern of the case. "By its plain language," the Fourth Circuit announced, "§ 230 creates a federal immunity to *any* cause of action that would make service providers liable for information originating with a third-party user of the service."[100] Without getting into the details of the CDA's legislative history,[101] the Fourth Circuit attributed a clear goal and rationale based on freedom of speech: "Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning internet medium."[102] The Fourth Circuit even added the key word "broad" to statutory language:

> Fearing that the specter of liability would therefore deter service providers from blocking and screening offensive material, Congress enacted §230's *broad* immunity "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material."[103]

Furthermore, the Fourth Circuit attempted to assign a global meaning to Section 230 by insisting that "Section 230 represents the approach of Congress to a problem of national and international dimension."[104] While

---

[96] *Id.* at 329.

[97] *Id.*

[98] *Id.* at 330.

[99] *Id.*

[100] *Id. See also* David R. Sheridan, Note, *Zeran v. AOL and the Effect of Section 230 of the Communications Decency Act upon Liability for Defamation on the Internet*, 61 ALB. L. REV. 147 (1997) (discussing *Zeran*'s holding).

[101] The *Zeran* case was argued in front the Fourth Circuit on October 2, 1997, and its decision was reached on November 12, 1997. A few months before the *Zeran* case, the CDA was challenged in the United States Supreme Court, which decided on June 26, 1997, to strike down most of the CDA as a violation of the First Amendment. Reno v. ACLU, 521 U.S. 844 (1997).

[102] *Zeran*, 129 F.3d at 330 (emphasis added).

[103] *Id.* at 331 (emphasis added) (citing 47 U.S.C. § 230(b)(4)).

[104] *Id.* at 334.

the *Zeran* decision was widely questioned by commentators,[105] on June 22, 1998, the Supreme Court of the United States denied certiorari,[106] which ended the legal uncertainty.

Other federal courts soon found the value of *Zeran* and followed its direction. In *Blumenthal v. Drudge*,[107] the Federal District Court for the District of Columbia faced a defamation case against AOL. Here, as the provider of an interactive computer service, AOL contended that it only disseminated content provided by someone else who authored the defamatory statement under § 230(c)(1). However, the author of the defamatory statement, Matt Drudge, was an AOL contractor.[108] After a long quote from *Zeran*, the district court ruled that AOL entitled to Section 230 immunity, following *Zeran*.[109] A similar question was raised in *Ben Ezra, Weinstein, & Co. v. America Online Inc.*[110] Here, the Tenth Circuit faced a defamation and negligence complaint by plaintiff, a publicly traded company, against AOL for incorrect information concerning plaintiff's stock price and share volume. AOL, which disseminated stock information concerning more than 40,000 publicly traded stocks and securities through its Quotes & Portfolios service, argued that two independent third-party companies provided the information. The Tenth Circuit concluded that "[i]mposing liability on [AOL] for the allegedly inaccurate stock information provided by [third-party] would 'treat' [AOL] as the 'publisher or speaker,' a result § 230 specifically proscribes."[111]

Zeran gained momentum in May 2002, when a congressional committee confirmed the rulings.[112] In 2003, *Zeran* spread to the Third and

---

[105] *E.g.*, Sewali K. Patel, *Immunizing Internet Service Providers from Third-Party Internet Defamation Claims How Far Should Courts Go?*, 55 VAND. L. REV. 647, 679–89 (2002); Susan Freiwald, *Comparative Institutional Analysis in Cyberspace The Case of Intermediary Liability for Defamation*, 14 HARV. J.L. & TECH. 569, 594–96 (2001); Brian C. McManus, *Rethinking Defamation Liability for Internet Service Providers*, 35 SUFFOLK U. L. REV. 647, 659 (2001); Annemarie Pantazis, Zeran v. America Online, Inc. *Insulating Internet Service Providers from Defamation Liability*, 34 WAKE FOREST L. REV. 531, 547–50 (1999); Michelle J. Kane, *Internet Service Providers' Liability* Blumenthal v. Drudge, 14 BERKELEY TECH. L. J. 483, 498–500 (1999).

[106] Zeran v. Am. Online, Inc., 524 U.S. 937, 937 (1998).

[107] Blumenthal v. Drudge, 992 F. Supp. 44, 46 (D.D.C. 1998).

[108] *Id.* at 51.

[109] *Id.*

[110] Ben Ezra, Weinstein, & Co. v. Am. Online Inc., 206 F.3d 980, 986 (10th Cir. 2000).

[111] *Id.* at 986.

[112] "The courts have correctly interpreted section 230(c), which was aimed at protecting against liability for such claims as negligence . . . and defamation. . . . The Committee intends these interpretations of section 230(c) to be equally applicable to those entities covered by H.R. 3833."

Seventh Circuits.[113] The Ninth Circuit also embraced *Zeran* in 2003, though in a puzzling way. The first case in the Ninth Circuit was *Batzel v. Smith*, where plaintiff brought defamation complaints against both the author of the defamatory statement, as well as the operator of website and listservs.[114] The key here was that the author emailed the statement to the operator of the website, without knowing that the message would be posted on the website. It was the website operator who chose the message and edited it before posting it online. Was the website operator an "information content provider" under § 230(c)(1)? The Ninth Circuit was split on this issue. The majority decided to add some conditions to the standard *Zeran* category:

> [A] service provider or user is immune from liability under § 230(c)(1) when a third person or entity that created or developed the information in question furnished it to the provider or user under circumstances in which a reasonable person in the position of the service provider or user would conclude that the information was provided for publication on the Internet or other "interactive computer service."[115]

Judge Gould, dissenting in part with the majority, believed that the majority went too far.[116] For Judge Gould,

> [The court] should hold that the CDA immunizes a defendant only when the defendant took no active role in selecting the questionable information for publication. If the defendant took an active role in selecting information for publication, the information is no longer 'information provided by another' within the meaning of § 230.[117]

By that standard, Judge Gould suggested, the defendant "is not entitled to CDA immunity because [defendant] actively selected Smith's e-mail message for publication."[118]

H.R. REP. NO. 107-449, at 13 (2002), *reprinted in* 2002 U.S.C.C.A.N. 1741, 1749 (citation omitted). H.R. 3833 was later passed as the Dot Kids Implementation and Efficiency Act of 2002, Pub. L. No. 107-317, 116 Stat. 2766.

[113] In 2003, two other federal circuit courts joined the Fourth Circuit in following the *Zeran* decision. *See* Green v. Am. Online, 318 F.3d 465, 470–71 (3rd Cir. 2003) (failure to police its network). It took some more time for other circuit courts to join them. *See* Almeida v. Amazon.com, 456 F.3d 1316, 1321–24 (11th Cir. 2006); Johnson v. Arden, 614 F.3d 785, 791–92 (8th Cir. 2010) (website host sued for defamatory statements posted on an internet discussion board).

[114] Batzel v. Smith, 333 F.3d 1018, 1022 (9th Cir. 2003).

[115] *Id.* at 1034.

[116] *Id.* at 1036–41 (Gould, J., concurring in part, dissenting in part).

[117] *Id.* at 1038.

[118] *Id.* at 1040.

Despite their differences, the majority and the dissent in *Batzel* shared a common goal which was to reject the categorical approach in *Zeran*. They suggested a case-by-case approach as an alternative to the bright-line rule adopted by *Zeran*. Nevertheless, the Ninth Circuit was unwilling to question the *Zeran* approach directly.[119]

Less than two months later, the Ninth Circuit delivered the opinion for *Carafano v. Metrosplash* (2003), where the Court yielded to *Zeran* completely. Here, a third-party user of MetroSplash.com, a dating service website, impersonated actress Christiane Carafano and created a profile on the website without the latter's knowledge nor consent. The question was whether the website was entitled to § 230(c) immunity. The trial court, a district court for the Central District of California, considered MetroSplash an "information content provider" thus not entitled to immunity because of its involvement in creating the profile through its application and questionnaire.[120] The Ninth Circuit disagreed. Here, the Ninth Circuit conceded to the *Zaren* reading of Section 230, and acknowledged, for the first, time, that "courts have treated § 230(c) immunity as quite robust, adopting a relatively expansive definition of 'interactive computer service' and a relatively restrictive definition of 'information content provider.'"[121] Based on that general direction from *Zaren*, the Ninth Circuit came up with its own formula, "[u]nder the statutory scheme, an 'interactive computer service' qualifies for immunity so long as it does not also function as an 'information content provider' for the portion of the statement or publication at issue."[122] It repeated the sweeping statement: "so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity regardless of the specific editing or selection process."[123]

In sum, by the mid-2000s, federal courts had formed a consensus in adopting a broad reading of Section 230, transforming the federal statute to a fundamental legal framework for the internet era. More recently,

---

[119] Later, the Ninth Circuit characterized its decision in *Batzel* as "join[ing] the consensus developing across other courts of appeals that § 230(c) provides broad immunity for publishing content provided primarily by third parties." Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003).

[120] Carafano v. Metrosplash.com, Inc., 2072 F. Supp. 2d 1055, 1066–68 (C.D. Cal. 2002).

[121] Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003).

[122] *Id.* at 1123.

[123] *Id.* at 1124. In another case, the question was whether a suit against web-based social media network MySpace was barred by the CDA when its negligence in failing to verify the age of a girl creating an account led to sexual assault by a predator. Doe v. MySpace, Inc., 528 F.3d 413, 422 (5th Cir. 2008).

Section 230 was interpreted broadly in terms of its geographic coverage.[124] Both the Second Circuit and the Ninth Circuit reasoned that since the primary purpose of Section 230 is to limit liability, thus it will limit liability regardless.[125] As a result, Section 230 immunity, so far as digital platforms are acting as publishers,[126] is now global for U.S. courts.

2. Material Contribution

In some other cases, however, the role of the digital platform or service provider cannot be avoided, even by a broad reading of Section 230. In these cases, a notion of "material contribution" was developed. In *Fair Housing Council v. Roommate.com*,[127] the question was whether an online roommate-matching website was entitled to Section 230 immunity, despite the fact that it allegedly violated the Fair Housing Act (FHA) for discriminatory information. The trial court followed *Carafano* and ruled that Roommate was protected by immunity.[128] On appeal, the Ninth Circuit panel was split.[129] In April 2008, the Ninth Circuit reheard the matter *en banc*. The *en banc* Court was split. The majority, led by Judge

---

[124] *See* Force v. Facebook, Inc., 934 F.3d 53, 74 (2nd Cir. 2019); Gonzalez v. Google, 2 F.4th 871, 888 (9th Cir. 2021). The facts of these two cases are similar. In both cases, victims of overseas terrorist attacks filed suits against digital platforms for their roles in terrorist groups' recruitment and propagation of terror. *Force*, 934 F.3d at 57; *Gonzalez*, 2 F.4th at 880. Platforms claimed Section 230 immunity. *Force*, 934 F.3d at 62; *Gonzalez*, 2 F.4th at 882. Plaintiffs argued that that Section 230 did not explicitly cover territory outside the United States, in accordance with the doctrine of presumption against extraterritoriality. *Force*, 934 F.3d at 62; *Gonzalez*, 2 F.4th at 882. Both the Second and Ninth Circuits rejected this claim. *Force*, 934 F.3d at 74; *Gonzalez*, 2 F.4th at 912–13.

[125] The Second Circuit ruled that Section 230's "primary purpose is limiting civil liability in American courts." *Force*, 934 F.3d at 74. Because litigation of civil claims occurs in the United States courts, presumption against extraterritoriality is no barrier to the application of Section 230. *Id.* at 74. The Ninth Circuit closely followed the reasoning of the Second Circuit when it stated "because § 230(c)(1) focuses on limiting liability, the relevant conduct occurs where immunity is imposed, which is where Congress intended the limitation of liability to have an effect, rather than the place where the claims principally arose." *Gonzalez*, 2 F.4th at 888.

[126] In *Gonzalez*, the Ninth Circuit left one issue open: plaintiffs argued for liability on a theory that Google generated revenue by selling advertising space through its AdSense program, thus Google shared the revenue with users on the latter's videos. 2 F.4th at 898. The Ninth Circuit ruled Section 230 did not cover it. *Id.* According to the Ninth Circuit, the plaintiffs' revenue-sharing allegations "are not directed to the publication of third-party information. These allegations are premised on Google providing ISIS with material support by giving ISIS money." *Id.*

[127] Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1164 (9th Cir. 2008) (en banc).

[128] Fair Hous. Council v. Roommate.com, LLC, No. CV 03–09386PA, 2004 WL 3799488, at *6 (C.D. Cal. Sept. 30, 2004).

[129] Fair Hous. Council v. Roommates.com, LLC, 489 F.3d 921 (9th Cir. 2007), *vacated en banc*, 521 F.3d 1157 (9th Cir. 2008).

Alex Kozinski, found that CDA immunity did not apply to Roommate in two aspects. First, when users create a personal profile on its website, Roommate's questionnaire asked for information on race and sexual orientation, which may have violated the FHA.[130] The majority believed that "[t]he CDA does not grant immunity for inducing third parties to express illegal preferences."[131] Roommate became an information content provider under Section 230, because "Roommate's own acts—posting the questionnaire and requiring answers to it—are entirely its doing and thus section 230 of the CDA does not apply to them."[132] Second, after registration, Roommate creates a personal profile and user's discriminatory preferences are displayed on her profile page; and Roommate even let users search its database.[133] The majority ruled that Roommate became "much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information."[134] The majority considered the search function problematic as it was "similarly designed to steer users based on discriminatory criteria."[135] In that aspect, according to the majority, it differs materially from generic search engines such as Google, Yahoo! and MSN Live Search.[136] Here the majority adopted a "material contribution" standard equivalent to the role of an editor who makes the "affirmative decision to publish," "so he contributes materially to its allegedly unlawful dissemination. He is thus properly deemed a developer and not entitled to CDA immunity."[137]

The dissent, led by Judge McKeown, however, argued *Carafano* controlled here,[138] and believed the majority's opinion created an "unprecedented expansion of liability for internet service providers [which] threatens to chill the robust development of the internet that Congress envisioned."[139] Guided by a broad reading of Section 230 immunity, the argument continued, regardless of what Roommate did, it was "the users [who] have furnished this information to Roommate for

---

[130] Fair Hous. Council v. Roommates.com, 521 F.3d at 1164.
[131] *Id.* at 1165.
[132] *Id.* at 1165.
[133] *Id.* at 1167.
[134] *Id.* at 1166.
[135] *Id.* at 1167.
[136] *Id.* at 1167.
[137] *Id.* at 1171.
[138] *Id.* at 1186 (McKeown, J., concurring in part, dissenting in part) ("*Carafano* presented circumstances virtually indistinguishable from those before us. . . .").
[139] *Id.* at 1176.

Roommate to publish in their profiles."[140] "The profile is created solely by the user, not the provider of the interactive website. Indeed, without user participation, there is no information at all."[141] This position gained support in *Kimzey v. Yelp! Inc.*, where Judge McKeown led a unanimous panel holding that Yelp's rating system, based on user's inputs, "is best characterized as the kind of neutral tool operating on voluntary inputs," therefore covered by Section 230 immunity.[142]

The "material contribution" test, which initially targeted the design and function of a website or app, later became a test of the behavior of the website operator. In *FTC v. Accusearch, Inc.*, the website operator "solicited requests for confidential information protected by law, paid researchers to find it, knew that the researchers were likely to use improper methods, and charged customers who wished the information to be disclosed."[143] In *Huon v. Denton*, the Seventh Circuit commented that "[a] company can . . . be liable for creating and posting, inducing another to post, or otherwise actively participating in the posting of a defamatory statement in a forum that that company maintains."[144] In *Jones v. Dirty World*, the Sixth Circuit ruled that, though the operator of the website selected the statements for publication, he had not "materially contributed to the defamatory content" because he did not author them.[145] The Sixth Circuit's ruling makes "material contribution" meaningless as a judicial scrutiny by returning to the "publisher" and "distributor" distinction.

3. Notification

As can be seen in Part II, all jurisdictions outside the United States treat notification as a decisive factor in deciding negligence on the side of the digital platforms or service provider. Notification is also raised by plaintiffs from time to time in American courts. The first test came to the federal court right after Section 230 was enacted, in *Zeran v. America Online, Inc.*[146] Zeran argued that the fact that he had notified AOL of the

---

[140] *Id.* at 1185.

[141] *Id.* at 1182.

[142] Kimzey v. Yelp! Inc., 836 F.3d 1263, 1270 (9th Cir. 2016). Similarly, the Fourth Circuit found a consumer review website was covered by Section 230 immunity. Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 591 F.3d 250, 260 (4th Cir. 2009).

[143] FTC v. Accusearch, Inc., 570 F.3d 1187, 1201 (10th Cir. 2009).

[144] Huon v. Denton, 841 F.3d 733, 742 (7th Cir. 2016).

[145] Jones v. Dirty World Ent. Recordings LLC, 755 F.3d 398, 415 (6th Cir. 2014).

[146] *See* Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997).

defamatory statements on the AOL bulletin board and AOL had not removed them made it *negligence*, regardless of Section 230 immunity to publishers.[147] The Fourth Circuit was not convinced: "Zeran simply attaches too much importance to the presence of the distinct notice element in distributor liability."[148] The Court concluded: "Liability upon notice would defeat the dual purposes advanced by § 230 of the CDA."[149] In *Universal Communication v. Lycos, Inc.*, the First Circuit joined other courts that have held that Section 230 immunity applies even after notice of the potentially unlawful nature of the third party content.[150] In *Barnes v. Yahoo*, plaintiff Cecilia Barnes broke off a lengthy relationship with her boyfriend, who then responded by posting profiles of Barnes on a website run by Yahoo.[151] Barnes notified Yahoo to remove the profiles, and the latter promised removal. However, Yahoo did not remove them until after Barnes filed the complaint in court. Barnes argued in court that although it may have had no initial responsibility to act, once Yahoo undertook to act, it must do so reasonably.[152] The Ninth Circuit did not find this persuasive. According to the court:

> [T]he duty that Barnes claims Yahoo violated derives from Yahoo's conduct as a publisher—the steps it allegedly took, but later supposedly abandoned, to de-publish the offensive profiles. It is because such conduct is publishing conduct that we have insisted that section 230 protects from liability.[153]

The Ninth Circuit was conscious that, after *Fair Housing*, it was following a "careful exegesis of the statutory language" rather than resting on a "broad statement of immunity."[154] Nevertheless, the court's reading of Section 230 is still broad because it refused to consider whether Yahoo was a publisher—therefore within the protection of Section 230—is changed by notification.

When there is no promise made to remove harmful content, then Section 230 becomes a complete defense. One example is *Klayman v. Zuckerberg*,[155] where an anti-Semitic hate-speech page created by a third-

---

[147] *Id.* at 332.
[148] *Id.*
[149] *Id.* at 333.
[150] Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 420 (1st Cir. 2007).
[151] Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1096 (9th Cir. 2009).
[152] *Id.* at 1102.
[153] *Id.* at 1103.
[154] *Id.* at 1100.
[155] Klayman v. Zuckerberg, 753 F.3d 1354, 1355 (D.C. Cir. 2014).

party user appeared on Facebook, and plaintiff Larry Klayman complained that Facebook did not remove the page timely. The D.C. Circuit found that Facebook was entitled to immunity under Section 230. The court commented that to the extent that Klayman did not claim breach of contract, his case could not be saved.[156] Similarly, the Second Circuit ruled in *Ricci v. Teamsters Union Local 456* that without a promise made to a user, the website owner who refused to remove defamatory contents was protected by Section 230.[157]

In sum, Section 230 cases reflect a strong judicial policy of providing a broad, generous immunity to digital platforms and service providers. This broad Section 230 immunity, when combined with a demanding personal jurisdiction requirement, makes court less accessible for millions of internet users. Other jurisdictions, however, adopt a very different legal approach. The remainder of this Article will demonstrate that, outside of the United States, other jurisdictions uniformly make their courts more accessible. This is achieved by extending the jurisdiction of their courts, adopting negligence standard for digital platforms' liabilities, and increasingly embracing global injunctions as remedies for civil liabilities.

II. GLOBALIZATION OF JURISDICTION

The first area of judicial divergence is jurisdiction. In contrast with the "minimum contacts" standard based on effect plus targeting, courts in Australia, the United Kingdom, Canada, the European Union, Japan, and China tend to treat effect as a decisive factor in asserting jurisdiction. As a result, internet users in these jurisdictions are able to file suit in their local court against service providers or even their digital platforms in California. Ironically perhaps, "globalization of jurisdiction,"[158] an American idea, is more readily embraced elsewhere.

A. COMMONWEALTH COUNTRIES

The first defamation case arising from the internet in Australia was *Gutnick v. Dow Jones*, filed in November 2000 by Joseph Gutnick

---

[156] *Id.* at 1359.

[157] Ricci v. Teamsters Union Local 456, 781 F.3d 25, 28 (2d Cir. 2015) (holding that a suit against a website owner who refused to remove defamatory newsletters was barred by CDA).

[158] Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PA. L. REV. 311, 321 (2002) (arguing for a community-based cosmopolitan pluralist conception of jurisdiction).

against Dow Jones at the Supreme Court of Victoria (SCV, the trial court).[159] The legal issue regarded where the defamatory statement was made. Plaintiff Gutnick alleged that an article published in *Barrons* magazine—as well as on the *Wall Street Journal*'s website, WSJ.com—contained defamatory content. Gutnick was a resident in the State of Victoria, Australia, while Dow Jones was a Delaware company with its principal place of business in New York; the server of the website was in South Brunswick, New Jersey. Justice Hedigan of SCV ruled that the trial court had personal jurisdiction and thus granted writ to serve the process outside of Australia. Dow Jones thus appeared in SCV court and challenged the jurisdiction. The trial court dismissed the summons. Both the Court of Appeals in Victoria and the federal High Court of Australia affirmed the ruling.[160]

Dow Jones argued in the trial court that internet publication occurred when and where the material was uploaded to the server.[161] The trial court disagreed and held that "publication takes place where and when the contents of the publication . . . are seen and heard . . . and comprehended by the reader or hearer."[162] Therefore, the court concluded, libel "was published in the State of Victoria when downloaded by Dow Jones subscribers."[163] The Australian High Court agreed. Following Justice Dixon's statement in *Lee v. Wilson & Mackinnon*,[164] Chief Justice Gleeson concluded that "[i]t is where that person downloads the material that the damage to reputation may be done. Ordinarily then, that will be the place where the tort of defamation is committed."[165]

What was particularly interesting in the *Gutnick* case was the underlying dialogue with the U.S. law—a commentator called it "negotiating [the] American legal hegemony."[166] Justice Hedigan, the trial

---

[159] *Gutnick v Dow Jones & Co Inc* [2001] VSC 305 (28 August 2001) (Austl.).

[160] *Dow Jones & Co Inc v Gutnick* [2001] VSCA 249 (21 September 2001) (Austl.); *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 (10 December 2002) (Austl.).

[161] *Gutnick*, [2001] VSC 305, para. 21 (28 August 2001) ("It is not to be doubted that the core submission of the defendant is that the Internet publication of 'Unholy Gains' occurred when and where the material was uploaded in New Jersey, that is, when it was pulled from the server in New Jersey.").

[162] *Id.* para. 60.

[163] *Id.*

[164] Lee v. Wilson & Mackinnon, [1934] HCA 60, (1934) 51 CLR 276, 287 ("It is the publication, not the composition of a libel, which is the actionable wrong." Justice Dixon). *Gutnick*, [2002] HCA 56, para. 25.

[165] *Id.* para. 44.

[166] Brian Fitzgerald, Dow Jones & Co Inc v Gutnick: *Negotiating American Legal Hegemony' in the Transnational World of Cyberspace*, 27 MELB. UNIV. L. REV. 590, 610 (2003).

judge, found that the United States Supreme Court decision in *Calder* supported his conclusion on finding jurisdiction.[167] He was not moved when Dow Jones "remind[ed] me more than once that I held the fate of freedom of dissemination of information on the Internet in my hands."[168] Justice Hedigan describes the position insisted on by Dow Jones as "[t]o say that the country where the article is written, edited and uploaded and where the publisher does its business, must be the forum is an invitation to entrench the United States, the primary home of much of Internet publishing, as the forum."[169] The *Gutnick* decision was the first act of revolt against the U.S. hegemony—ruling against a major American corporation and asserted jurisdiction on jurisprudence in defiance of the U.S. law.

In England, the *Gutnick* decision was fully embraced as an update of the English common law.[170] The English Court of Appeal considered in 2004 that *Gutnick* brought English common law to the internet age.[171] Even Dow Jones has clearly accepted the position, and in a subsequent case, it did not even bother to challenge the English court's jurisdiction.[172]

In Canada, the Supreme Court of British Columbia came close to embracing the *Gutnick* decision in *Crookes v. Yahoo* in 2007.[173] Here, defendant Yahoo had neither physical presence nor bank accounts in British Columbia. Yahoo offered a service called "Yahoo! Groups," which enabled users to create topic-oriented online discussion groups. One such group was "GPC-Members Group" a forum about the Green Party of Canada. Access to postings and information was restricted to individuals who were invited by the manager of the Group, and not available to the

---

[167] *Gutnick*, [2001] VSC 305, para. 57.

[168] *Id.* para. 44.

[169] *Id.* para. 73.

[170] Shortly before the *Gutnick* decision in Australia, Dow Jones had a similar case in England. *See* Chadha & Osicom Techs. Inc. v. Dow Jones & Co. Inc. [1999] EWCA (Civ) 1415 (Eng.). The *Forbes* magazine had a similar case, which was litigated all the way to the House of Lords. *See* Berezovsky v. Michaels and Others, Glouchkov v. Michaels and Others [2000] UKHL 25, [2000] (appeals taken from Eng.). However, both cases were decided based on the print version of the newspaper or magazine, without touching the issue of online libel.

[171] Lennox Lewis & Others v. Don King [2004] EWCA (Civ) 1329 [29] (appeal taken from Eng.) ("In *Gutnick v Dow Jones* the High Court of Australia firmly rejected a challenge, in the context of Internet libel, to the applicability of such established principles as that vouchsafed in *Duke of Brunswick*."). *Duke of Brunswick* was an 1849 decision by the Queen's Bench. The Duke of Brunswick v. Harmer (1849) 117 Eng. Rep. 75, 14 Q.B. 185.

[172] Dow Jones & Co. Inc. v. Jameel [2005] EWCA (Civ) 75 [16] (Eng.) ("Dow Jones made no challenge to English jurisdiction.").

[173] Crookes v. Yahoo, 2007 BCSC 1325 (Can.) (B.C.), *aff'd*, Crookes v. Yahoo, 2008 BCCA 165 (Can) (B.C.).

general public. Plaintiff, Wayne Crookes, was not a member of the GPC-Members Group, and filed a complaint against Yahoo alleging certain postings made by the GPC-Members Group defamed him. Yahoo challenged the jurisdiction of the court by arguing that "[i]n order for this court to assume jurisdiction over Yahoo, there must be a real and substantial connection between the cause of action against Yahoo and British Columbia."[174] The court was ready to embrace *Gutnick*, by stating that "[w]ith respect to internet communications, the site of the alleged defamation is where the damage to reputation occurs." Citing *Gutnick*, it continued: "It is when a person downloads the impugned material from the internet that the damage to the reputation may be done, and it is at that time and place that the tort of defamation is committed."[175] However, the court found such allegations missing in the plaintiff's pleadings: "Mr. Crookes must show that alleged defamatory postings on the GPC-Members website, hosted by Yahoo on servers outside British Columbia, were accessed, downloaded and read by someone in British Columbia, thereby damaging his reputation in British Columbia. Mr. Crookes has neither alleged nor tendered any evidence. . . ."[176]

This is one step further than the same court went in *Wiebe v. Bouchard*, when the court announced that it had jurisdiction in libel cases even if the defamatory libel posted on a Canadian Government's website was authored by Quebec residents in Quebec.[177] The Supreme Court of Canada has not spoken directly on *Gutnick*, but it has taken notice of the case with approval in *Society of Composers v. Canadian Association of Internet Providers*, and considered it part of the "broader context" in its discussion of online copyright infringement.[178]

Courts in Commonwealth countries responded to the arrival of the internet by adopting a nuanced notion of "publication" in defamation cases, which is functionally closer to the "effect" theory in the United States. By eliminating the need for "targeting," they made courts more accessible to millions of users.

---

[174] Crookes v. Yahoo, 2007 BCSC 1325, para. 28 (Can.) (B.C.).

[175] *Id.* para. 26.

[176] *Id.* para. 29.

[177] Wiebe v. Bouchard, 2005 BCSC 47, paras. 33, 39 (Can.) (B.C.). *See also* Burke v. NYP Holdings Inc., 2005 BCSC 1287 (Can.) (B.C.).

[178] Canadian Ass'n of Internet Providers v. Soc'y Composers, Authors & Music Publishers Canada, 2004 SCC 45, para. 41 (Can.).

B. EUROPEAN UNION

The European Union has developed a similar doctrine since the arrival of the internet. Like the "publication" notion in Commonwealth countries, EU law was centered on the "effect," with the primary concern being how to make courts accessible. Before the arrival of the internet, the Brussels Convention,[179] Article 2 provided the general rule: persons domiciled in a contracting state shall, whatever their nationality, be sued in the courts of that state.[180] However, there is special jurisdiction, which allows, under Article 5(3), a person domiciled in a contracting state to be sued in another contracting state, in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred.[181] In *Bier v. Mines de Potasse d'Alsace, SA*,[182] the European Court of Justice (ECJ) interpreted Article 5(3) as giving a plaintiff the option to file a lawsuit either in the courts based on where the damage occurred, or in the courts of the place where the event giving rise to the damage occurred.

In *Shevill v. Presse Alliance SA*,[183] a defamation case brought by residents in England against a French newspaper, the ECJ applied the doctrine in *Mines de Potasse d'Alsace* and interpreted that "the place of the event giving rise to the damage" in a defamation case "can only be the place where the publisher of the newspaper in question is established, since that is the place where the harmful event originated and from which the libel was issued and put into circulation."[184] This made the ECJ consistent with the common law tradition.[185] Here, like in *Mines de Potasse d'Alsace,* the European Court of Justice reiterated that the option was given to the plaintiff: "Although there are admittedly disadvantages to having different courts ruling on various aspects of the same dispute, the plaintiff always has the option of bringing his entire claim before the

---

[179] Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, July 28, 1990, 1990 O.J. (C 189) arts. 2, 3. [hereinafter the Brussels Convention]. Signatories of the 1990 Brussels Convention include Belgium, Germany, France, Italy, Luxembourg, and the Netherlands.

[180] *Id.* art. 2.

[181] *Id.* art. 5, para. 3.

[182] Case 21/76, Handelskwekerij G.j. Bier B.V. v. Mines de Potasse d'Alsace, S.A., 1976 E.C.R. 1735, 1748.

[183] Case C-68/93, Shevill v. Presse All. S.A., 1995 E.C.R. I-450. *See also* Shevill v. Presse All. S.A. [1996] AC 959 (HL) (appeal taken from Eng.).

[184] Case C-68/93, Shevill v. Presse All. S.A., 1995 E.C.R. I-450, ¶ 24.

[185] Douglas W. Vick & Linda Macpherson, *Anglicizing Defamation Law in the European Union*, 36 VA. J. INT'L L. 933, 937 (1996).

courts either of the defendant's domicile or of the place where the publisher of the defamatory publication is established."[186]

The question of internet publication, however, is how to define the place where the harmful event occurred. This was the question in *eDate Advertising/Martinez*.[187] Here, the plaintiff domiciled in Germany.[188] He had been sentenced to life imprisonment for a murder case but was released on parole in 2008. Defendant eDate Advertising was an Austrian company operating a website publishing news, which included a report on plaintiff's case.[189] Plaintiff brought an action before a German court, seeking an order from the court that the defendant refrain from using his full name when reporting about the case. The main legal issue was whether a German court had jurisdiction over an Austrian company.[190] The German Federal Court of Justice (the Bundesgerichtshof) stayed proceedings and referred the case to Court of Justice of the European Union ("CJEU").[191]

The CJEU acknowledged the difficulty created by the internet—distribution of defamatory statements became world-wide in the online world, thus traditional tools such as distribution of hard copies became less useful.[192] In the new context, the CJEU reasoned, the objective remained the same, that is to make sure that "a person who has suffered an infringement of a personality right by means of the internet may bring an action in one forum in respect of all of the damage caused, depending on the place in which the damage caused in the European Union by that infringement occurred."[193] In order to achieve this goal, the CJEU came up with a new conceptual tool—the "center of interest." According to the CJEU:

> Given that the impact which material placed online is liable to have on an individual's personality rights might best be assessed by the court of the place where the alleged victim has his center of interests, the

---

[186] *Shevill*, 1995 E.C.R. ¶ 32.
[187] Joined Cases C-509/09 & C-161/10, eDate Advert. GmbH v. X & Martinez v. MGN Ltd., 2011 E.C.R. ¶ 19.
[188] *Id.* ¶ 15.
[189] *Id.* ¶ 16.
[190] *Id.* ¶ 18.
[191] *Id.* ¶ 24.
[192] *Id.* ¶ 47.
[193] *Id.* ¶ 48.

> attribution of jurisdiction to that court corresponds to the objective of the sound administration of justice. . . .[194]

The court did not elaborate on the "center of interests," but acknowledged that "[t]he place where a person has the center of his interests corresponds in general to his habitual residence."[195] It indicates that other factors, such as professional activity, may be relevant in considering the "center of interests." This ruling is, in general, consistent with the Commonwealth countries' practice of protecting the plaintiff's interest in ensuring a forum is available for their grievances.[196]

In 2017, the CJEU explained the "center of interest" in *Bolagsupplysningen v. Handel*.[197] In this case, Bolagsupplysningen, an Estonian company, brought a defamation action in Estonian court against Svensk Handel, a Swedish trade association, for publishing incorrect information on the latter's website.[198] The alleged defamation was that Svensk Handel included Bolagsupplysningen in a "blacklist" on their website based on accusations of fraud and deceit.[199] The question for the Estonian court was whether it had jurisdiction over a foreign corporation for defamation published in Swedish.[200] The Riigikohus (the Supreme Court, Estonia) referred the case to the CJEU.[201]

Article 7(2) of Regulation No. 1215/2012 provides that a person domiciled in a Member State may be sued in another Member States "in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur."[202] Following the CJEU's decision in *eDate Advertising*, the parties agreed that Estonia was not the place where the event giving rise to the damage occurred. So, the question

---

[194] *Id.*

[195] *Id.* ¶ 49.

[196] Jan-Jaap Kuipers, *Towards a European Approach in the Cross-Border Infringement of Personality Rights*, 12 GERMAN L.J. 1681, 1697 (2011); Jan Oster, *Rethinking* Shevill *Conceptualising the EU Private International Law of Internet Torts Against Personality Rights*, 26 INT'L REV. L. COMPUTS. & TECH. 113, 118 (2012); Lorna Gillies, *Jurisdiction for Cross-Border Breach of Personality and Defamation* Edate Advertising *and* Martinez, 61 INT'L & COMP. L.Q. 1007, 1010–11 (2012).

[197] Case C-194/16, Bolagsupplysningen v. Handel, ECLI:EU:C:2017:766, ¶ 33 (Oct. 17, 2017).

[198] *Id.* ¶ 9.

[199] *Id.* ¶ 10.

[200] *Id.* ¶ 11.

[201] *Id.* ¶ 21.

[202] Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (recast), O.J. (L 351) 1, 7(2).

for the CJEU was whether Estonian courts had jurisdiction by virtue of being the courts of the place where the alleged damage occurred.[203]

In order to answer the question, the CJEU recalled that in *eDate Advertising*, the person who considers that her rights have been infringed "must have the option of bringing an action for damages, in respect of all the harm caused, before the courts of the Member State in which the center of [her] interests is based."[204] However, in this case, because the victim of alleged internet defamation is a legal person (corporate entity)

> Article 7(2) of Regulation No. 1215/2012 must be interpreted as meaning that a legal person claiming that its personality rights have been infringed by the publication of incorrect information concerning it on the internet and by a failure to remove comments relating to that person can bring an action for rectification of that information, removal of those comments and compensation in respect of all the damages sustained before the courts of the Member State in which its centre of interests is located.[205]

Because of the "centre of interests," the CJEU rejected the suggestion that Article 7(2) means that a person can bring an action "before the courts of each Member State in which the information published on the internet is or was accessible."[206]

In sum, the notion of "center of interest," created by the European Court of Justice in response to the arrival of the internet, is essentially an elaboration of "effect" theory under *Calder*. It serves the same purpose as the elaboration of "publication" in Commonwealth courts, that is, to make court open to the millions of internet users.

C. JAPAN

Since the Meiji era, Japan followed continental Europe closely in developing its civil code and civil procedure.[207] Not surprisingly, lawmakers and the courts in Japan responded to the arrival of the internet like the European Union. In Japan, an online defamation case in the

---

[203] *Handel*, Case C-194/16, ¶ 30.

[204] *Id.* ¶ 32.

[205] *Id.* ¶ 44.

[206] *Id.*

[207] Kohji Tanabe, *The Process of Litigation An Experiment with the Adversary System*, *in* LAW IN JAPAN: THE LEGAL ORDER IN A CHANGING SOCIETY 73, 77 (Arthur Taylor von Mehren ed., 1963). A major revision was made to the Code of Civil Procedure in 1996. *See* Yasuhei Taniguchi, *The Development of an Adversary System in Japanese Civil Procedure*, *in* LAW IN JAPAN: A TURNING POINT 80, 81, 92 (Daniel H. Foote ed., 2007).

Supreme Court of Japan in 2016, the *Universal* case,[208] had a striking resemblance with the CJEU decision in *Handel*. In this 2016 Japanese case, one of the plaintiffs, Universal Entertainment Corporation (Universal), a Japanese corporation which manufactured, developed, and distributed a gaming machine, was founded, and controlled by entrepreneur Kazuo Okada.[209] Universal had a wholly owned subsidiary Aruze Gaming America, Inc., incorporated in the State of Nevada in the United States.[210] Aruze owned 20 percent of the defendant company's (Wynn Resort Ltd.) shares, which operated a casino in Nevada.[211]

In early 2012, Wynn Resort alleged that Okada had engaged in improper activities in the Philippines in violation of the United States Foreign Corruption Practice Act (FCPA) and decided in a board meeting to oust Aruze as a shareholder. The next day, the board meeting resolution—including a statement on Okada's alleged violation of FCPA—was posted on the defendant company's website. The statement was in English. While defendant company and Aruze were engaged in litigation in Nevada courts,[212] Universal filed an internet defamation complaint against the defendant company in Tokyo District Court in August 2012.[213] The central question was whether courts in Japan had jurisdiction.

On March 10, 2016, the Supreme Court of Japan (SCJ) decided that this was one of the "special circumstances" under Article 3-9 of the Japanese Code of Civil Procedure where Japanese courts should *not* exercise jurisdiction. The final result is seemingly similar to the CJEU's

---

[208] *See* Saikō Saibansho [Sup. Ct.] Mar. 10, 2016, 2014 (Ju) 1985, SAIKŌ SAIBANSHO MINJI HANREISHŪ [Minshu] 1, https://www.courts.go.jp/app/hanrei_en/detail?id=1450 [https://perma.cc/2B3U-RAP6] [hereinafter Universal].

[209] *Id.* While the disputes originated in the state of Nevada, the parties were engaged in litigation in courts in Japan, as well as state courts in Nevada. Okada v. The Eighth Judicial District Court, 131 Nev. 834, 359 P.3d 1106 (2015). After the Supreme Court of Japan's 2016 ruling, the parties continued their disputes in both Nevada state courts and federal courts. *See* Wynn Resorts, Ltd. v. The Eighth Judicial District Court, 133 Nev. 369, 399 P.3d 334 (Nev. 2017); Okada v. The Eighth Judicial District Court, 134 Nev. 6, 408 P.3d 566 (Nev. 2018). In federal court the case was *Universal Entertainment Corp. v. Aruze Gaming America, Inc.*, Case No. 2:18-cv-00585-RFB-NJK, 2020 WL 2840153 (D. Nev. May 30, 2020).

[210] Universal, *supra* note 208; Okada v. The Eighth Judicial District Court, 359 P.3d at 1109 (Nev. 2015).

[211] Universal, *supra* note 208.

[212] *Supra* note 209.

[213] Universal, *supra* note 208.

decision in *Handel*.[214] However, a closer examination shows that the SCJ was more aggressive in claiming jurisdiction. Article 3-9 provides:

> Even when the Japanese courts have jurisdiction over an action . . . , the court may dismiss the whole or part of an action without prejudice if it finds that there are special circumstances (*tokubetsu no jijō*, 特別の事情) because of which, if the Japanese courts were to conduct a trial and reach a judicial decision in the action, it would be inequitable to either party or prevent a fair and speedy trial, in consideration of the nature of the case, the degree of burden that the defendant would have to bear in responding to the action, the location of evidence, and other circumstances.[215]

From its text, it is clear that Article 3-9 functions like the doctrine of *forum non conveniens* in the United States,[216] by recognizing that the court has jurisdiction, but should exercise its discretion, and decline to exercise that jurisdiction. Therefore, the SCJ implied that Japanese courts did have jurisdiction in a situation like this.

The legal foundation for jurisdiction in Japan, the Code of Civil Procedure Article 3-3 (viii),[217] is similar to Article 7(2) of the EU Regulation No. 1215/2012.[218] What reason led the SCJ to conclude that Japanese courts had jurisdiction in a case where defendant company

---

[214] *See* Case C-194/16, Bolagsupplysningen v. Handel, ECLI:EU:C:2017:766, ¶¶ 30, 44 (Oct. 17, 2017).

[215] MINJI SOSHŌHŌ [Minsohō] [C. CIV. PRO.] 1996, art. 3-9 (Japan), *translated in* CODE OF CIVIL PROCEDURE (Japanese L. Translation [JLT DS]), http://www.japaneselawtranslation.go.jp/law/detail/?id=2834&vm=04&re=02&new=1 [https://perma.cc/EF92-4BJ6] (last updated Mar. 22, 2012).

[216] *See* Koji Takahashi, *The Jurisdiction of Japanese Courts in a Comparative Context*, 11 J. PRIV. INT'L L. 103, 104, 121, 127 (2015); Koji Takahashi, *Japan's Newly Enacted Rules on International Jurisdiction With a Reflection on Some Issues of Interpretation*, 13 ANN. PRIV. INT'L L. 146, 156 (2011). *See generally* Sinochem Int'l Co. Ltd. v. Malaysia Int'l Shipping Corp., 549 U.S. 422 (2007) (discussing the doctrine of *forum non conveniens*). In this aspect, Japan differs from other civil law countries who largely consider *forum non conveniens* inconsistent with civil law legal systems. *See* RONALD A. BRAND, SCOTT R. JABLONSKI, FORUM NON CONVENIENS: HISTORY, GLOBAL PRACTICE, AND FUTURE UNDER THE HAGUE CONVENTION ON CHOICE OF COURT AGREEMENTS 124–25 (Oxford 2007) (discussing *forum non conveniens* in Japan).

[217] An action may be filed with the Japanese courts in the case of "an action for tort: if the place where the tort occurred is within Japan (excluding if the consequences of a wrongful act committed in a foreign country have arisen within Japan but it would not ordinarily have been possible to foresee those consequences arising within Japan)." MINJI SOSHŌHŌ [Minsohō] [C. CIV. PRO.] 1996, art. 3-3(viii) (Japan), *translated in* CODE OF CIVIL PROCEDURE (Japanese L. Translation [JLT DS]), http://www.japaneselawtranslation.go.jp/law/detail/?id=2834&vm=04&re=02&new=1 [https://perma.cc/LDD3-3QLV].

[218] Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (recast), O.J. (L 351) 1, 7(2).

posted the statement (in English) on its website in Nevada, alleging violation of U.S. law? The only reason would be because of what the Supreme Court of Estonia asked the CJEU in *Handel*: the website is accessible everywhere in the world, therefore the court of the place the website is accessible has jurisdiction because that is the place where the damage occurred.[219] In *Handel*, the CJEU did not endorse such a broad approach; it adopted the "center of interest" theory to set limits on jurisdiction.[220] The SCJ achieved the same result as the CJEU did in *Handel*, but through its discretion under the *forum non conveniens* doctrine.

Japan's legal framework for international jurisdiction is relatively new—it was introduced in 2011 when the Code of Civil Procedure was amended.[221] Japan closely follows the European Union when taking part in the discussions and negotiations at the Hague Conference on Private International Law.[222] On the question of jurisdiction in tort cases, it has been consistent with the 1968 Brussels Convention, the 1990 Brussels Convention, and the 1999 Draft Convention.[223] The language choice in Article 3-3(viii), "action relating to torts" is understood as *locus delicti commissi* (where a tort was committed). It came from Article 5(ix) of the same Code of Civil Procedure, which is for allocating court jurisdiction in

---

[219] *See Handel*, Case C-194/16 ¶¶ 30, 44.

[220] *See supra* text accompanying notes 194–206. In 2005, the European Court of Justice ruled that *forum non conveniens* was inconsistent with the Brussels Convention in Owusu v. Jackson, Case C-281/02, Grand Chamber of the European Court of Justice, Mar. 1, 2005. *See* Gilles Guniberti, *Forum Non Conveniens and the Brussels Convention*, 54 INT'L & COMP. L.Q. 973 (Oct. 2005).

[221] *Act for Partial Revision of Code of Civil Procedure and Civil Provisional Remedies Act*, 54 JAPANESE Y.B. INT'L L. 723, 723 (2011), *incorporated in* MINJI SOSHŌHŌ [Minsohō] [C. CIV. PRO.] 1996, art. 3-9 (Japan), *translated in* CODE OF CIVIL PROCEDURE (Japanese Law Translation [JLT DS]), http://www.japaneselawtranslation.go.jp/law/detail/?id=2834&vm=04&re=02&new=1 [https://perma.cc/8BGK-P6X8]. *See generally* Masato Dogauchi, *New Japanese Rules on International Jurisdiction General Observation*, 54 JAPANESE Y.B. INT'L L. 260 (2011) (discussing the drafting history of the amendment).

[222] Yuko Nishitani, *International Jurisdiction of Japanese Courts in a Comparative Perspective*, 60 NETH. INT'L L. REV. 251, 253 (2013). Japan started taking part in the Hague Conference on Private International Law (HCCH) from 1904 (Meiji 37) as a non-European participant. *See* Masato Dogauchi & Keisuke Takeshita, *Japan's Participation in the Hague Conference of Private International Law Based on Historical Sources*, 7 ANN. PRIV. INT'L L. 140, 142 (2005).

[223] *See* Preliminary Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters, Hague Conference on Private International Law, art. 10, Oct. 30, 1999, Prel. Doc. 11. (2000), https://assets.hcch.net/docs/638883f3-0c0a-46c6-b646-7a099d9bd95e.pdf [https://perma.cc/76JG-3JXE].

domestic contexts.[224] The language 'the place where the tortious act occurred,' (*fuhōkōi ga attachi*, 不法行為があった地) includes two elements: first, the place where a tortious act is committed (*kagai kōi chi,* 加害行為地), and second, the place where the consequence of the tort is felt (*kekka hasse chi*, 結果発生地).[225] Traditionally, in Japan, it was understood that *either* element could satisfy the jurisdictional requirement.[226] So what the SCJ did in the *Universal* case, by relying on Article 3-9, was to declare that the Japanese courts had jurisdiction, but that it was a wise exercise of discretion to not claim it.

In sum, the SCJ's emphasis of discretion under the *forum non conveniens* doctrine in deciding jurisdiction is functionally similar to the CJEU's notion of "center of interest." What is equally amazing is that the SCJ, which is not considered as active by American standards, is providing a key function like the CJEU in the European Union, in Japan's response to the arrival of the internet.

D. CHINA

As mentioned earlier, China differs from the first camp (the United States) and the second camp (the Commonwealth countries, the European Union, and Japan) in terms of political censorship, and in denying global digital platforms access to its domestic market. Inside the Chinese market, however, the structure is quite similar—national digital platforms, such as Alibaba, Baidu, and Tencent, dominate the national market but they are concentrated in mega cities such as Beijing, Shenzhen,

---

[224] Nozomi Tada [多田望], *International Civil Jurisdiction Based on the Place of the Tort*, 55 JAPANESE Y.B. INT'L L. 287, 288 (2012). Article 5 of the Civil Procedure Code provides that "An action set forth in one of the following items may be filed with the court of jurisdiction in the place specified in said item: . . . (ix) an action for a tort: the place where the tort took place . . ." MINJI SOSHŌHŌ [Minsohō] [C. CIV. PRO.] 1996, art. 5 (Japan), *translated in* CODE OF CIVIL PROCEDURE (Japanese Law Translation [JLT DS]), http://www.japaneselawtranslation.go.jp/law/detail/?id=2834&vm=04&re=02&new=1 [https://perma.cc/7L9B-KTUU].

[225] Tada, *supra* note 224, at 297–98.

[226] Tada states:

> In practice, in determining international jurisdiction under Article 5(ix), Japanese courts had recognized that both the place of act and the place of consequence were equivalent and thus the plaintiff was entitled to sue the defendant at either place. Accordingly, if either was located in Japan, jurisdiction of the Japanese courts was recognized on the basis of the place where the tort was committed.

Id. at 299.

and Hangzhou.[227] Internet users across China also need to access local courts for civil litigation. When these cases are not considered politically sensitive, Chinese lawmakers and courts adopt similar rules to Japan and the European Union in making courts accessible.

Wang Shen v. Google, one of the early cases of online copyright disputes, was a copyright dispute between Google and author Wang Shen decided by the Beijing No.1 Intermediate People's Court in December 2011.[228] Wang alleged that Google and the operator of its China domain website, www.Google.cn, infringed upon her copyrights by digitizing one collection of her popular short novels and making the book available on that website to its users without the author's permission.[229] Google questioned the jurisdiction of the court by suggesting that digitization of the book occurred in California because it was stored in a server in California.[230] The Beijing Court did not find the argument convincing.[231] The Beijing Court stated: "the place where the tort act occurred" (*qinquan xingwei di*, 侵权行为地), according to the interpretation of the PRC Supreme People's Court,[232] included both the place where the tort is committed (*shishi di*, 实施地) and the place where results occurred (*jieguo*

---

[227] Alibaba is headquartered in Hangzhou, Zhejiang province. *Company Overview*, ALIBABA GROUP, https://www.alibabagroup.com/en/about/overview [https://perma.cc/339Y-FSXQ] (last visited Nov. 21, 2021). Tencent is headquartered in Shenzhen, Guangdong province. *About Us*, TENCENT, https://www.tencent.com/en-us/about.html#about-con-1 [https://perma.cc/A4QW-ZNYD] (last visited Nov. 21, 2021). Baidu was founded on January 1, 2000, in Beijing. *Our Company*, BAIDU, https://home.baidu.com/home/index/company [perma.cc/X6EM-449N] (last visited Dec. 1, 2021).

[228] Wangshen yu Beijing Guxiang Xinxi Jishu Youxian Gongsi deng Zhuzuoquan Quanshu Qinquan Jiufen Yishen Minshi Panjueshu (王莘与北京谷翔信息技术有限公司等著作权权属侵权纠纷 审民事判决书) [Wang Shen v. Google Inc.], Beijing 01 Civ. 1321 Case No. 2011 (Beijing No.1 Interm. People's Ct. Dec. 20, 2012), *aff'd*, Guge Gongsi yu Wangshen Qinhai Zhuzuoquan Jiufen'an (谷歌公司与王莘侵害著作权纠纷上诉案) [Google Inc. v. Wang Shen], High Civ. 1221 Case No. 2013 (Beijing People's High Court Dec. 19, 2013). The decision by Beijing People's High Court was selected by the PRC Supreme People's Court as one of the "2013 Top 10 Innovative Intellectual Property Cases." *Top 10 Innovative Intellectual Property Cases in Chinese Courts in* 2013, SUPREME PEOPLE'S COURT OF THE PEOPLE'S REPUBLIC OF CHINA, http://zscq.court.gov.cn/alfx/201404/t20140425_195316.html [https://perma.cc/CR3N-4XWN].

[229] Wang Shen v. Google Inc., *supra* note 228.

[230] *Id.*

[231] *Id.*

[232] Zhonghua Renmin Gongheguo Minshi Susongfa (中华人民共和国民事诉讼法) [Civil Procedure Law of the People's Republic of China] (promulgated by the National People's Congress, Apr. 9, 1991, amended by the Standing Committee of the 12th National People's Congress, June 27, 2017) P.R.C. Laws, Apr. 9, 2001, at art. 28, http://www.npc.gov.cn/zgrdw/englishnpc/Law/2007-12/12/content_1383880.htm [https://perma.cc/57CS-NV76] [hereinafter Database of Laws and Regulations].

fashengdi, 结果发生地). "Therefore, if any one of those places is in China, Chinese courts have jurisdiction over the whole dispute."[233]

With the rapid increase in the online population, online defamation is a rapidly developing area.[234] On June 23, 2014, the Supreme People's Court issued a guideline on online tortious cases, "Supreme People's Court Rules on Several Issues in Tort Cases Related to Personality Rights" (2014 SPC Rule).[235] Article 2 of this 2014 SPC Rule renders a general norm in the context of online torts:

> Actions based on allegations of online infringement of personality rights may be brought to the people's court where the infringement occurred, or where the defendant is domiciled.
>
> The place where infringement occurred includes the place where computer terminals involved in the alleged infringement is located; the place where infringement results occurred includes the domicile of the plaintiff.[236]

Since the 2014 SPC Rule, courts across the country have applied the rule in deciding cases involving China's best known internet companies. Baidu, China's search engine, is domiciled in Beijing, but it is sued by plaintiffs all over the country in defamation cases.[237] In these cases, Baidu typically challenges the jurisdiction of the local courts. It argues that by virtue of Baidu being domiciled in Beijing, and the fact that its servers are located in Beijing, only the local court in Beijing should

---

[233] Wang Shen v. Google Inc., *supra* note 228.

[234] *See generally* Yan Mei Ning, *Internet Intermediary Liability in Online Defamation Lawsuits The Case of Mainland China*, 11 J. COMP. L. 283 (2016) (analyzing online defamation cases in China); Xin He & Fen Lin, *The Losing Media? An Empirical Study of Defamation Litigation in China*, 230 CHINA Q. 371 (2017) (surveying 524 defamation cases in China); Benjamin L. Liebman, *Innovation through Intimidation An Empirical Account of Defamation Litigation in China*, 47 HARV. INT'L L.J. 33 (2006) (surveying 223 defamation cases in China).

[235] Zuigao Renmin Fayuan Guanyu Shenli Liyong Xinxi Wangluo Qinhai Renshen Quanyi Minshi Jiufen Anjian Shiyong Falü Ruogan Wenti de Guiding (最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定) [Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Cases involving Civil Disputes over Infringements upon Personal Rights and Interests through Information Networks] (promulgated by the Supreme People's Court, No. 11, June 23, 2014, effective Oct. 10, 2014) [hereinafter 2014 SPC Rule].

[236] *Id.* art. 2.

[237] The case, *infra* note 238, was a ruling by the court in Shanghai. Courts in other areas ruled similarly. For example, the Chongqing No.5 Intermediate People's Court in its decision (2019) 渝 05 民辖终 680 号 on June 17, 2019 affirmed the lower court's decision that it had jurisdiction over Baidu in a defamation dispute. Another court, the Harbin Intermediate People's Court (Heilongjiang province, Northern China) ruled in its decision (2019) 黑 01 民辖终 275 号 on August 1, 2019, that the local district court had jurisdiction over Baidu in a defamation dispute.

have jurisdiction. These challenges are typically dismissed. For example, in *Baidu v. Jiang Li*,[238] plaintiff Ms. Jiang Li, a resident in Shanghai's Yangpu District, brought her online defamation complaint against Baidu in Yangpu District Court. The trial court dismissed Baidu's challenge to its jurisdiction, thus Baidu appealed to the Shanghai No.2 Intermediate People's Court, the appellate court. The appellate court concluded:

> [I]n this defamation dispute, the [general] rule is that local courts where defendant is domiciled or [the] court of the place where infringement occurred shall have jurisdiction. In online infringement cases, the place where infringement occurred includes the place where computers and other information processing equipment are located; the place where infringement results occurred include the domicile of the plaintiff who alleges the infringement. In this case, the plaintiff was a resident in Shanghai Yangpu District, and the Yangpu District Court had proper jurisdiction. The dismissal by the District Court on jurisdiction was not an error. We hereby affirm. Baidu's reasons for appeal are not substantiated, therefore [it] is dismissed.[239]

In sum, China adopted a similar rule in embracing the "effect" theory, like the courts in Japan, the European Union, and the Commonwealth countries. By not requiring a "targeting" element to satisfy jurisdiction, all the jurisdictions outside the United States diverge from it by making their courts accessible to local internet users.

III. LIABILITY OF THE INTERNET INTERMEDIARIES

The second area of judicial divergence is the liability of digital platforms or internet service providers (ISPs). In the United States, as has been shown in Part I, the regulatory approach is one of broad immunity under Section 230, characterized by a bright-line distinction between "publisher" and "distributor."[240] By contrast, there is no such broad immunity beyond the borders of the United States. In the United Kingdom and other Commonwealth countries like Australia, and Hong Kong, a theory of "innocent dissemination" offers some protection, like the Directive on Electronic Commerce in the EU or a special statute in Japan limiting the liability of ISPs. But all these countries in the Second Camp keep tort liability by examining the behavior of the ISP rather than relying

---

[238] Beijing Baidu Wangxun Keji Youxian Gongsi yu JiangLi Mingyuquan Jiufen Ershen Minshi Caidingshu (北京百度网讯科技有限公司与江　名誉权纠纷二审民事裁定书) [Baidu v. Jiang Li] Hu 02 Civ. 237 (Shanghai No. 2 Interm. People's Ct. Mar. 29, 2019).

[239] *Id.*

[240] *See* discussion *supra* text accompanying notes 88–91.

on its status. China adopts a similar tort liability approach, which allows Chinese users to hold ISPs accountable.

A. COMMONWEALTH COUNTRIES

In the United Kingdom, the question of "publisher" was considered in an internet defamation case in 1999, *Godfrey v. Demon Internet Ltd.*[241] Here, defendant Demon Internet was an ISP that hosted an online newsgroup that published postings by users.[242] The plaintiff, a customer, found one posting defamatory and notified the Defendant. Defendant acknowledged receipt of the notice but did not remove the content until after the posting expired.[243] The legal issue was focused on whether the defendant was a publisher or not. Judge Morland, writing for the English High Court, stated:

> After the 17th January 1997 after receipt of the Plaintiff's fax the Defendants knew of the defamatory posting but chose not to remove it from their Usenet news servers. In my judgment this places the Defendants in an insuperable difficulty so that they cannot avail themselves of the defense provided by [law].[244]

Judge Morland continued:

> At Common Law liability for the publication of defamatory material was strict. There was still publication even if the publisher was ignorant of the defamatory material within the document. Once publication was established the publisher was guilty of publishing the libel unless he could establish, and the onus was upon him, that he was an innocent disseminator.[245]

Judge Morland surveyed American cases and quoted *Cubby*, *Stratton Oakmont*, and *Zeran* in great detail. He noted: "[i]n my judgment the English 1996 Act did not adopt this approach or have this purpose."[246]

The second case was *Bunt v. Tilley*.[247] Judge Eady, after considering *Godfrey*, was not sure that *Godfrey* could be applied directly.

---

[241] Godfrey v. Demon Internet Ltd [2000] 3 WLR 1020 (QB) (Morland J.) (Eng.).

[242] *Id.* para. 11.

[243] *Id.*

[244] *Id.* para. 20.

[245] *Id.* para. 26.

[246] *Id.* para. 45.

[247] Bunt v. Tilley [2006] EWHC (QB) 407, [2007] 1 WLR 1243 (Eng.). *See also* Grant v. Google UK Ltd. [2005] EWHC (Ch) 3444; Jameel (Yousef) v. Dow Jones & Co. Inc. [2005] EWCA (Civ) 75, [2005] 2 WLR 1614 (UK).

The judge was reasoning along the line of the "innocent dissemination" doctrine when he commented:

> What was left open for later consideration was how a court in England should approach a situation where, by contrast with the factual situation in Mr. Godfrey's case, an ISP had truly fulfilled no more than a passive role as owner of an electronic device through which defamatory postings were transmitted.[248]

Judge Eady continued:

> [F]or a person to be held responsible there must be knowing involvement in the process of publication of *the relevant words.* It is not enough that a person merely plays a passive instrumental role in the process.[249]

Judge Eady applied the same rule in *Metropolitan International Schools Ltd. v. Designtechnica Corp.*[250] In the lower court, Judge Eady applied the same rule in *Tamiz v. Google*.[251]

On appeal, however, the English Court of Appeal showed a different assessment in its ruling in 2013.[252] Lord Justice Richards stated that it was wrong for the trial judge to regard Google's role "as a purely passive one."[253] The Lord Justice clarified that the doctrine of "innocent dissemination" was conditioned by the fact that the publisher did not know the publication was defamatory. But notification changed that condition. The Lord Justice stated:

> [I]f Google Inc allows defamatory material to remain on a Blogger blog after it has been notified of the presence of that material, it might be inferred to have associated itself with, or to have made itself

---

[248] *Bunt,* [2006] EWHC 407 (QB), para. 14. The doctrine of "innocent dissemination" was first articulated in *Emmens v. Pottle*, (1885) 16 QBD 354, 357 (Eng.), where Lord Esher, M.R. ruled that a vendor who sold newspapers that contained libel in it was not liable if he can prove that he, as a "innocent disseminator," did not know that it contained a libel. In *Vizetelly v. Mudie's Select Library Ltd.*, [1900] 2 QB 170 (Eng.), the Court of Appeal, relying on *Emmens*, ruled that proprietors of a circulating library who circulated and sold a book that contained a libel was liable because they were not able to prove they did not know the libel. RACHAEL MULHERON, PRINCIPLES OF TORT LAW 808–09 (2nd ed. 2020).

[249] *Bunt*, [2006] EWHC 407 (QB), para. 23.

[250] Metro. Int'l Schs. Ltd. v. Designtechnica Corp. [2009] EWHC (QB) 1765, [2011] WLR 1743 (Eady J) (Eng.).

[251] Tamiz v. Google Inc. [2012] EWHC (QB) 449 (Eady J) (Eng.).

[252] Tamiz v. Google Inc. [2013] EWCA (Civ) 68, [2013] 1 WLR 2151 (Eng.).

[253] *Id.* para. 23.

> responsible for, the continued presence of that material on the blog and thereby to have become a publisher of the material.[254]

The Court of Appeal's position might have been stimulated by Judge Parkes in his decision in *Davison v. Habeeb*,[255] a case decided three months prior to Judge Eady's ruling in *Tamiz*. The 2011 case is quite similar to *Tamiz*. Here, Google, as one of the defendants, was brought to the court for defamatory postings on its platform Blogger.com. Google was represented by Antony White, [256] the same counsel who had represented Google in *Metropolitan*, making similar arguments. But Judge Parkes differed from Judge Eady on the assessment of Google's role: "Eady J.'s observations in *Bunt v. Tilley* about the need for a mental element were made in the context of ISPs which were no more than passive conduits which connected one person or one computer with another."[257] Judge Parkes pointed out, "[i]n the present case," however, Google "provides and hosts a platform which is designed to enable users to publish what (within limits) they wish by making their material available for others to access and download."[258]

To make the point clearer, Judge Parkes highlighted an additional element: "Moreover, [Google] appears to assume a degree of responsibility for what is published on its Blogger.com platform. . . . The ability to remove offending words is plainly a highly relevant factor."[259] A few lines later, Judge Parkes repeated this:

> I do not think that the voluntary removal of some articles pending the outcome of the proceedings establishes that [Google] is in any sense the editor of the material, but I do accept that the ability to take down offensive material is a relevant factor in determining whether it is a publisher.[260]

In Hong Kong, the Court of Final Appeal, the highest judicial authority in Hong Kong, reached the same conclusion in *Oriental Press v. Fevaworks Solutions*.[261]

In Australia, a series of cases were filed against Yahoo and Google between 2010 and 2012. In February 2010, Milorad Trkulja, a resident of

---

[254] *Id.* para. 34.
[255] Davison v. Habeeb & Ors [2011] EWHC (QB) 3031 (Parkes J) (Eng.).
[256] *Id.* para. 3.
[257] *Id.* para. 39.
[258] *Id.*
[259] *Id.*
[260] *Id.* para. 40.
[261] Oriental Press Grp. Ltd. v. Fevaworks Sols. Ltd., [2013] 16 H.K.C.F.A.R. 366 (C.F.A.) (H.K.).

Victoria, brought suit against Google.[262] After some procedural issues in 2010 and 2011,[263] the legal issue focused on the question of whether Google was a "publisher."[264] Google's defense was that it was not a publisher because it had no knowledge of the defamatory statements.[265] In addition, Google argued there should be "immunity" for an internet search engine.[266] On appeal, the Court of Appeals in Victoria (VSCA) reversed and ruled in favor of Google.[267] The High Court of Australia (HCA), however, endorsed the trial court's opinion that "it is strongly arguable that Google's intentional participation in the communication of the allegedly defamatory results of Google search engine users supports a finding that Google published the allegedly defamatory results."[268] It also corrected the VSCA by making it clear that the plaintiff, in the pleading stage, was not required to plead the degree of Google's involvement in the publication "for the reason that all degrees of participation in the publication are publication."[269] The HCA did not discuss the issue of immunity. This is most likely because the issue was not appealed. It is notable that both the trial court and VSCA rejected the notion. The VSCA, in its decision in favor of Google, stated:

---

[262] *Trkulja v Google Inc LLC [No. 1]* [2010] VSC 226 (27 May 2010) (Austl.). During this period, similar complaints against Google were brought to the courts in New South Wales and South Australia. *See Bleyer v Google Inc* [2014] NSWSC 897 (12 August 2014); *Duffy v. Google Inc* [2015] SASC 170 (27 October 2015); *Google Inc v Duffy* (2017) 129 SASR 304 (Austl.).

[263] *Trkulja v Google Inc [No. 2]* [2010] VSC 490 (3 November 2010), ¶ 17; *Trkulja v Google Inc [No. 3]* [2011] VSC 503 (5 October 2011), ¶ 6; *Trkulja v Google Inc [No. 4]* [2011] VSC 560 (3 November 2011), ¶¶ 2–3.

[264] *Trkulja v Google Inc [No. 5]* [2011] VSC 560 (12 November 2012), ¶¶ 16–18; *Trkulja v Google Inc [No. 6]* [2015] VSC 635 (17 November 2015).

[265] *Trkulja [No. 5]*, [2011] VSC, ¶ 15.

[266] *Trkulja [No. 6]*, [2015] VSC, ¶ 72.

[267] *Google Inc v Trkulja [No.7]* (2016) 342 ALR 504, ¶ 415 (Austl.).

[268] *Trkulja v Google LLC [No.8]* [2018] HCA 25 (13 June 2018), ¶ 38 (Austl.).

[269] *Id.* ¶ 40. In a more recent case, *Fairfax Media Publications v. Voller*, the court was facing a similar issue—whether defendants who had public Facebook page containing defamatory content created by third-party users were publishers. [2021] HCA 27 (Sept. 8, 2021). Justices Gageler and Gordon, who were among the majority of High Court of Australia in this case, stated:

> [T]he word "intentionally" . . . should be understood to be directed at an intention to facilitate, or provide a platform for, communication of the allegedly defamatory matter. Enough for participation in a process that is in fact directed to making matter available for comprehension by a third party to be characterized as intentional is that the participation in the process is active and voluntary. That is irrespective of the degree of active and voluntary participation in the process. And it is irrespective of knowledge or intention on the part of the participant as to the defamatory content of the matter published.

Id. ¶ 66.

> The legislation [in America] has produced, on occasion, an unhappy result: *Carafano v. Metrosplash.com Inc*. The American experience suggests that the content in any Australian legislation would require much thought. But one thing, in our opinion, is clear. If there is to be any immunity in favor of a search engine from liability for defamation, it must be conferred by legislation.[270]

In sum, courts in the Commonwealth countries have universally rejected the notion of general immunity, but rather followed traditional common law in torts by adopting a negligence standard. Despite the efforts of Google and other American corporations, who have repeatedly urged them to adopt Section 230 immunity, these courts did not find it convincing, nor the power to do so.

B. EUROPEAN UNION

The European Union legal framework in the Directive on Electronic Commerce[271] is built upon traditional tort law. The Directive was largely formulated in late 1998,[272] deliberation ensued early in 1999, and it was passed by the European Parliament in June 2000.[273] Its immediate background was a series of cases on the question of liability of ISPs. In England, litigation of the *Godfrey v. Demon Internet Ltd.* case was still ongoing from early 1997 to March 1999.[274] In Germany, Mr. Felix Somm, director of the CompuServe Deutschland GmbH, the German subsidiary of CompuServe, was going through a criminal trial for the company's inadequate efforts to block pornography.[275] In May 1998, a Munich criminal court sentenced Somm to two years of imprisonment.[276] In France, on April 10, 2000, less than two months before the adoption of the Directive, LICRA, a French non-profit organization filed a complaint

---

[270] *Trkulja [No. 7]*, 342 ALR, ¶ 414.

[271] *See generally* Directive 2000/31/EC, of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), 2000 O.J. (L 178/1) (establishing a framework on electronic commerce).

[272] *Commission Proposal for a European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market*, COM (1998) 586 final (Nov. 18, 1998).

[273] *See* Graham Pearce & Nicholas Platten, *Promoting the Information Society The EU Directive on Electronic Commerce*, 6 EUR. L.J. 363, 367–68 (2000).

[274] *See* Godfrey v. Demon Internet Ltd. [1999] EWHC 244, [2001] QB 201 (Morland J) (UK).

[275] *See* Karl-Heinz Ladeur, *Monitoring and Blocking Illegal Content on the Internet — A German and Comparative Law Perspective*, 41 GERMAN Y.B. INT'L L. 55, 76 (1998); Lothar Determann, *The New German Internet Law*, 22 HASTINGS INT'L & COMP. L. REV. 113, 120 (1998).

[276] *See* Ladeur, *supra* note 275; Determann, *supra* note 275.

against Yahoo and Yahoo France at the Superior Court of Paris.[277] These cases showed how urgent the issue was for the European Union to formulate the legal framework; both the *Godfrey* case and the American statute, the Digital Millennium Copyright Act (DMCA) of 1998,[278] pointed in the direction of the reform they needed.

On ISP liability, there was nothing like CDA Section 230 in the European Union; rather, the Directive on Electronic Commerce adopted a soft safe-harbor notion. It imagined three categories of ISP functions: "mere conduit" under Article 12,[279] "caching" under Article 13,[280] and "hosting" under Article 14.[281] In general, an ISP is not liable for the information transmitted, stored, or posted by a third-party user if the ISP does not have actual knowledge of illegal activity or information, or if the ISP "upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."[282] Consistent with the notion of safe harbor, there is no general obligation for ISPs to monitor activities on their websites under Article 15.[283] Therefore, the Directive resembles the English approach, a tort-based approach, and in treating all torts—defamation, copyrights, trademarks, etc.—alike.

There are a small number of defamation cases based on Article 12, including the case of *Sotiris Papasavvas*.[284] Here the CJEU clarified that

> . . . the limitations of civil liability specified in Articles 12 to 14 of Directive 2000/13 do not apply to the case of a newspaper publishing company which operates a website on which the online version of a newspaper is posted . . . since it has knowledge of the information posted and exercises control over that information, whether or not access to that website is free of charge.[285]

---

[277] *See* Marc H. Greenberg, *A Return to Lilliput The* LICRA v. Yahoo *Case and the Regulation of Online Content in the World Market*, 18 BERKELEY TECH. L.J. 1191, 1192 (2003); Xavier Amadei, Note, *Standards of Liability for Internet Service Providers A Comparative Study of France and the United States with a Specific Focus on Copyright, Defamation, and Illicit Content*, 35 CORNELL INT'L L.J. 189, 220 (2001).

[278] The Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998) (DMCA). Section 202 of the DMCA amended the Copyrights Act by adding Section 512, which provides the notice and takedown rule, codified at 17 U.S.C. § 512 (2020).

[279] Council Directive 2000/31, art. 12 2000 O.J. (L 178) 12, 13.

[280] *Id.* art. 13.

[281] *Id.* art. 14.

[282] *Id.*

[283] *Id.* art. 15.

[284] Case C-291/13, Papasavvas v. O Fileleftheros Dimosia Etairia Ltd., ECLI:EU:C:2014:2209, ¶ 20 (Sep. 11, 2014).

[285] *Id.* ¶ 46.

Also,

> the exemptions from liability established in that directive cover only cases in which the activity of the information society service provider is of a merely technical, automatic and passive nature, which implies that that service provider has neither knowledge of nor control over the information which is transmitted or stored (citation omitted). [286]

The trademark case in *Google v. Louis Vuitton*[287] was on Google's "AdWords" referring service and the sponsored links in its search results. Louis Vuitton, owner of the luxury goods trademark, learned in 2003 that a search of its trademarks on Google triggered the display of "sponsored links" leading to websites offering imitation versions of Vuitton's products.[288] In February 2005, a Regional Court in Paris found Google liable, and the ruling was affirmed by the Court of Appeal in Paris in June 2006. The French Supreme Court (*"Cour de cassation"*) referred the issue to the CJEU. The CJEU found that the internet referencing service provider did not "use" the trademarks in the course of trade,[289] and thus cannot be held liable for directly infringing upon the trademarks. Therefore, the question became whether Google is liable for storing advertisers' information, or whether Article 14 is broad enough to exempt it.[290]

The CJEU had no doubt that Google's referring service satisfied the definition of "information society service,"[291] but that was only the beginning of the inquiry. The key for the CJEU is Google's *conduct*:

> In order for the storage by a referencing service provider to come within the scope of Article 14 of Directive 2000/13, it is . . . necessary that the conduct of that service provider should be limited to that of an "intermediary service provider" within the meaning intended by the legislature. . . .[292]

For this purpose, the CJEU continued, "it is necessary to examine whether the role played by that service provider is neutral, in the sense that its

---

[286] *Id.* ¶ 40.

[287] Joined Cases C-236/08 & C-238/08, Google France S.A.R.L. v. Louis Vuitton Malletier SA, 2010 E.C.R. I-2467.

[288] *Id.* ¶ 23.

[289] *Google France*, 2010 E.C.R., ¶ 58. The CJEU found that the advertisers who purchased Google's "AdWords" function to create sponsored links used the trademarks, and thus the trademarks proprietor was entitled to prohibit such use. *Id.* ¶¶ 72, 79, 99.

[290] *Id.* ¶ 106.

[291] *See id.* ¶ 110.

[292] *Id.* ¶ 112.

conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores."[293] The CJEU decided to leave the national courts to assess the facts,[294] but the general rule here is unmistakable:

> Article 14 of Directive 2000/13 must be interpreted as meaning that the rule laid down therein applies to an internet referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored.[295]

In the subsequent *L'Oréal v. eBay* case,[296] the CJEU followed *Google v. Louis Vuitton* closely. The question, whether eBay is protected by Article 14 of Directive 2000/13, depends on the role that eBay played:

> Where . . . the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of Directive 2000/31.[297]

In sum, the CJEU has consistently adopted a negligence standard in examining the conducts of ISPs and deciding liabilities, a clear contrast with the general immunity reflected in Section 230 of the CDA in the United States.

C. JAPAN

Japan's law on internet intermediary liability resembles that in the European Union. Better, it codified the norms in a separate statute. In November 2001, Japan enacted a law limiting civil liabilities of telecommunication service providers, known as the Provider Liability Limitation Act (プロバイダ責任制限法, PLLA), Act No. 137 of 2001.[298] Like

---

[293] *Id.* ¶ 114.

[294] *Id.* ¶ 119.

[295] *Id.* ¶ 120.

[296] *See* Case C-324/09, L'Oréal SA v. eBay Int'l AG, ECLI:EU:C:2011:474, ¶ 145 (July 12, 2011).

[297] *Id.* ¶ 116.

[298] Jouhou No Kaiji Nikansuru Hritsu [Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification

Section 230 of CDA in the United States, the PLLA provides general immunity to service providers. Article 3 of the Act provides that service providers, when they are not the creator of the content, "shall not be liable for any loss incurred from infringement."[299] The PLLA, however, departs from CDA Section 230; it resembles the EU's Directive on Electronic Commerce in adopting a tort approach by creating exceptions to general immunity. Under Article 3, exceptions are under two conditions: (1) it is technically possible to prevent transmission of such information, and (2) there is knowledge of such infringement.[300] Exceptions to general immunity apply if the service provider had had actual knowledge of the infringement or had adequate reasons to believe it caused such infringement.[301]

PLLA aimed to address issues emerging from judicial decisions prior to its enactment. One such issue is reflected in the *Nifty Forum* case by the Tokyo High Court, decided in September 2001.[302] In this defamation case, Nifty, a major ISP in Japan, operated a number of bulletin boards. One of the bulletin boards was "Modern Thought Forum," operated by Defendant B, a contractor called a sysop (シスオペ) (system operator) in Japan.[303] The sysop had the power to remove contents from the bulletin board. Plaintiff, a member of the Forum, learned about negative messages about her from her friends and notified the sysop by email to remove the defamatory contents, but the sysop refused.[304] The Tokyo District Court ruled in 1997 (before PLLA's enactment) that the sysop, as manager of Forum, is responsible for its smooth operation and owed a duty of care when notified of defamatory statements.[305] On appeal,

---

Information of the Senders], Act No. 137 of 2001, *translated in* (Japanese Law Translation [JLT DS]), http://www.japaneselawtranslation.go.jp (Japan) [https://perma.cc/2Q4Q-UELQ] [hereinafter Provider Liability Limitation Act]. *See generally* MASAO YANAGA, CYBER LAW IN JAPAN 199–200 (4th ed. 2020); Yoshihisa Hayakawa, *Japanese Law in the Era of the Internet The New and Coming Legislation in Japan*, 45 JAPANESE ANN. INT'L L. 61, 69–71 (2002).

[299] Provider Liability Limitation Act, art. 3.

[300] *Id.*

[301] *Id.*

[302] Tōkyō Kōtō Saibansho [Tokyo High Court] Sept. 5, 2001, Heisei 9 (ne) No. 2631, 2633, 2668, 5632, 1088 Hanrei Taimuzu [Hanta] 94 (Japan), *appealed from*, Tōkyō Chihō Saibansho [Tokyo Dist. Ct.] May 26, 1997, Heisei 6 (ne) 7784, 24828, 1610 Hanrei Jihō [Hanji] 22 (Japan) [hereinafter *Nifty Forum*]. *See generally* Hiroko Onishi, *The Online Defamation Maze Are We Finding a Way Out?*, 27 INT'L REV. L. COMPUTS. & TECH. 200, 203–04 (2013) (commenting on the *Nifty Forum* case); MASAO, *supra* note 298, at 197.

[303] Onishi, *supra* note 302, at 203.

[304] *Id.*

[305] 1610 HANREI JIHŌ [HANJI] 22.

the Tokyo High Court rejected this duty to remove defamatory statements. The High Court considered the sysop's power of removal based on the operation contract with the ISP; while it has the power of removal, it should also have the autonomy in making its decision based on its own assessments. The High Court ruled that the sysop did not breach its duty to remove the contents.[306]

PLLA was passed on November 30, 2001, a few months after the Tokyo High Court's decision.[307] The Japanese Diet, by contrast, did not adopt the high bar that the Tokyo High Court used in *Nifty Forum*. Instead, it gave some control to users by creating exceptions based on the knowledge of the ISP, namely, a negligence standard in Article 3.[308] In the *2 Channel* case,[309] the Tokyo High Court clearly followed the framework that PLLA sets. Here, the plaintiff was an animal hospital that found defamatory statements in the bulletin board operated by the defendant. Plaintiff notified the sysop, who refused to remove the defamatory statements because the latter did not think defamation was established. The Tokyo District Court, applying the newly enacted PLLA, found defamation was established and thus found the sysop liable for its failure to remove the content after notification.[310] The Tokyo High Court affirmed the decision. It also took the opportunity to clarify that a sysop's assessment of defamation should follow an assessment based on an "ordinary person's reading" (一般人の普通の注意). In doing so, the Tokyo High Court departed from its more deferential position to the ISPs.

---

[306] *Nifty Forum*, *supra* note 302.

[307] Provider Liability Limitation Act, *supra* note 298.

[308] *Id.* art. 3.

[309] Tōkyō Kōtō Saibansho [Tokyo High Court] Dec. 25, 2002, Heisei 14 (ne) No. 4083, 50 KŌTŌ SAIBANSHO MINJI HANREISHŪ [K MIN] (No. 3) 15; 1816 Hanrei jihō [Hanji] 52 (Japan).

[310] Tōkyō Chihō Saibansho [Tokyo Dist. Ct.] Jun. 26, 2002, Heisei 13 (wa) No.15125, SAIBANSHO SAIBANREI JŌHŌ [SAIBANSHOWEB], https://www.courts.go.jp/app/hanrei_jp/detail4?id=5818 [https://perma.cc/7ZF8-7KYV].

D. CHINA

Prior to the Civil Code,[311] the legal framework for liability of internet intermediaries in China was set by Tort Liability Law (2009).[312] Like the European Union, China adopted a fault-based tort liability for online infringement of civil rights. Article 36 provides:

> Internet users and Internet service providers (ISPs) shall bear tort liability if they utilize the Internet to infringe upon the civil rights of others.
>
> If an Internet user commits a tort through Internet services, the infringed shall be entitled to inform the ISP to take necessary measures, including, *inter alia*, deletion, blocking and disconnection. If the ISP fails to take necessary measures in a timely manner upon notification, it shall be jointly and severally liable with the said Internet user for the extended damage.
>
> If an ISP is aware that an Internet user is infringing on the civil rights and interests of others through its Internet services and fails to take necessary measures, it shall be jointly and severally liable with said Internet user for such infringement.[313]

Article 36 is largely based on the "note and takedown" in the United States Digital Millennium Copyright Act of 1998,[314] and notification doctrine is widely applied in online copyright and trademark infringement cases in China.[315] In the defamation realm, *Zhang Qin v. China.com*, was a case decided by Beijing Chaoyang District People's

---

[311] Zhonghua Renmin Gongheguo Minfadian (中华人民共和国民法典) (Civil Code of the People's Republic of China) (promulgated by the Nat'l People's Cong., May 28, 2020, effective Jan. 1, 2021), STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 2 (2020, Special Issue), *translated in* Database of Laws and Regulations, http://www.npc.gov.cn [https://perma.cc/VDH4-CZJP].

[312] Zhonghua Renmin Gongheguo Qinquan Zeren Fa (中华人民共和国侵权责任法) (Tort Liability Law of the People's Republic of China) (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 26, 2009, effective July 1, 2010, repealed January 1, 2021 by Article 1260 of the Civil Code, *id.*), http://www.gov.cn/flfg/2009-12/26/content_1497435.htm [https://perma.cc/Y8F7-9T8F], *translated in* Database of Laws and Regulations, http://www.npc.gov.cn [https://perma.cc/4RNW-GGLT].

[313] *Id.* art. 36. The substance of Article 36 is now provided in Articles 1194 and 1195 of the Civil Code, *supra* note 311.

[314] The Digital Millennium Copyright Act of 1998 (DMCA), *supra* note 278. The connection between Article 36 and DMCA was acknowledged in 张新宝 [Zhang Xinbao] and 任鸿雁 [Ren Hongyan], 互联网上的侵权责任：《侵权责任法》第 36 条解读 [*Tort Liability on the Web An Interpretation of Article 36 of Tort Liability Law*], 中国人民大学学报 [JOURNAL OF RENMIN UNIVERSITY OF CHINA] 17, 21 (2010, No.4).

[315] 周学峰 [Zhou Xuefeng] & 李平 [Li Ping], 网络平台治理与法律责任 [THE GOVERNANCE AND LIABILITY OF INTERNET INTERMEDIARY] 354, 35–69 (Beijing: 2018).

Court,[316] and affirmed on appeal by the Beijing No.3 Intermediate People's Court.[317] The defendant was Huawang Huitong (华网汇通), owner and operator of China.com, one of the earliest internet portals in China.[318] Plaintiff, a corporate executive of Sinopec Group, China's state-owned oil company, found defamatory messages targeting her on the bulletin board of China.com in 2003. She notified China.com on March 8, 2013, but heard nothing from them by March 15 of the same year when the plaintiff filed her complaint in court. During trial, the two sides did not dispute that the defamatory messages were composed and posted by third-party users; what was in question was whether the plaintiff had properly sent the notification to the defendant or not. The trial court had no difficulty dismissing the defendant's claims of no notification and found that the plaintiff had notified the defendant of the defamatory messages, but the defendant had failed to remove them in a timely manner. The district court announced:

> In accordance with the Article 36(2) of the Tort Law of the People's Republic of China, China.com is, together with the author of the messages, jointly and severally liable for the extended damage, namely, the damage caused from the date of plaintiff's notification to the date of removal.[319]

It is important to note that the Tort Law does not define "timely" removal nor "extended damage." In a code-based legal system like China's, this is where judicial discretion is exercised, and policy considerations are taken into account. In the *China.com* case, the District Court decided that one week after notification was enough to rule against the ISP.[320]

---

[316] Zhang Qin Yu Beijing Huawang Huitong Jishu Fuwu Youxian Gongsi Mingyu Quan Jiufen Yishen Panjue Shu (张琴与北京华网汇通技术服务有限公司名誉权纠纷 审民事判决书) [Zhang Qin v. China.com, Judgment of First Instance Court on A Dispute over Right of Reputation], China Judgments Online, https://wenshu.court.gov.cn [https://perma.cc/XD82-SB4K] (Beijing Chaoyang Dist. People's Ct., Oct. 23, 2013).

[317] Beijing Huawang Huitong Jishu Fuwu Youxian Gongsi Yu Zhang Qin Mingyu Quan Jiufen Ershen Panjue Shu (北京华网汇通技术服务有限公司与张琴名誉权纠纷二审民事判决书) [Zhang Qin v. China.com, Judgment of Second Instance Court on A Dispute over Right of Reputation], China Judgments Online, https://wenshu.court.gov.cn [https://perma.cc/ZQ7G-3KLK] (Beijing No.3 Interm. People's Ct., Mar. 31, 2014).

[318] China.com was founded in May 1999, according to its own website, https://www.china.com/zh_cn/general/about.html [https://perma.cc/EXS8-2X7R]. In July 1999, it became the first Chinese Internet business to be listed on NASDAQ in the United States. ZIXUE TAI, THE INTERNET IN CHINA: CYBERSPACE AND CIVIL SOCIETY 139 (2007).

[319] *Zhang Qin v. China.com*, *supra* note 317.

[320] *Id.*

In a more recent defamation case against zhihu.com (知乎),[321] a well-known blog in China, the Shanghai Xuhui District People's Court considered "timely" removal. Here, the plaintiff was a professor at Nanjing University who had his lawyer send zhihu.com a take-down notice after learning about defamatory messages posted on zhihu.com by third-party users.[322] The lawyer's letter was sent on June 12, 2019. Defendant removed one offensive message and subsequent comments by July 5, 2019. The trial court considered the removal timely, and that the defendant had met the "reasonable expectation" for ISPs.[323] With respect to another offensive message, however, defendant did not remove the offensive content until July 29, 2019, when the court proceedings had started. The trial court ruled that "defendant's action is beyond an ordinary person's reasonable expectation of 'timely removal,' thus defendant failed to take measures in timely manner."[324]

In sum, courts in Commonwealth countries, the European Union, Japan, and China universally adopt tort law negligence standard in deciding liability of internet intermediaries, despite their differences in legal traditions (common law vs. civil law), and political ideology (liberal democracy vs. authoritarianism).

IV. RISE OF GLOBAL INJUNCTION

The last area of judicial divergence is remedy. There cannot be a better factual pattern than that in *Hassell v. Bird*,[325] a recent California Supreme Court decision. The plaintiffs were attorneys who alleged defamatory content in consumer reviews posted on Yelp, which they suspected were authored by a former client.[326] They filed a lawsuit against the former client; the defendant did not appear in hearings, so the plaintiffs won a default judgment from the trial court. The trial court ordered the

---

[321] Long Yitao Yu Beijing Zhizhe Tianxia Keji Youxian Gongsi Mingyu Quan Jiufen Yishen Minshi Panjue Shu (龙亿涛与北京智者天下科技有限公司名誉权纠纷 审民事判决书) [Long Yitao v. Zhihu.com, Judgment of First Instance Court on A Dispute over Right of Reputation], Tianyan Cha (https://susong.tianyancha.com) (Shanghai Xuhui Dist. People's Ct., 2019), *aff'd*, Beijing Zhizhe Tianxia Yu Long Yitao Mingyu Quan Jiufen Ershen Panjue Shu (北京智者天下龙亿涛名誉权纠纷二审民事判决书) [Long Yitao v. Zhihu.com, Judgment of Second Instance Court on A Dispute over Right of Reputation] (Shanghai No.1 Interm. People's Ct., July 26, 2020).

[322] *Id.*

[323] *Id.*

[324] *Id.*

[325] Hassell v. Bird, 420 P.3d 776, 778 (Cal. 2018).

[326] *Id.* at 780.

defendant to remove defamatory reviews from Yelp.com. Because the court was not sure where the defendant was located, it also stated that "Yelp.com is ordered to remove all reviews posted by [defendant]."[327] Can a court issue an order on Yelp? The California Supreme Court ruled that Yelp is protected by Section 230 because the trial court's order essentially treated Yelp as a publisher.[328]

This Part analyzes similar cases litigated in courts in Commonwealth countries (United Kingdom and Canada), the EU, and Japan. In the U.K., a doctrine called *Norwich Pharmacal* created such a duty on an innocent third party, and now this doctrine has been applied to the internet. In the EU, the CEJU is more open to the idea of letting the court issue orders to ISPs which have an effect worldwide. Even Japan, in a recent case regarding Twitter by the Supreme Court of Japan, opens the possibility. China does not have judicial decisions on this issue yet. But China is actively exploring the idea of projecting its own judicial power beyond its borders. As a result, the U.S. digital platforms are increasingly facing the rise of global injunctions.

A. COMMONWEALTH COUNTRIES

In the nineteenth-century, an English court's power to issue injunction orders to a foreign corporation is fairly limited: the general rule is that an injunction would not be granted against a person who is not within the jurisdiction of the court, unless there is something to be done within the jurisdiction.[329] In order for a court to issue a global injunction order to an ISP, two barriers have to be overcome: the first is that an innocent third-party cannot be issued an injunction order; the second is that a non-resident innocent third-party is out of reach by the court. In the 1970s, the English court was breaking the first barrier. In 1973, the House of Lords ruled in the *Norwich Pharmacal* case that an innocent person may come under a duty to assist the injured person.[330] Here, patent owners and

---

[327] *Id.* at 781.

[328] *Id.* at 790, 792.

[329] FRANCIS TAYLOR PIGGOTT, SERVICE OUT OF THE JURISDICTION 31–36 (London, William Clowes & Sons, Ltd. 1892). However, this seemed still less rigid than the United States Supreme Court decision in *Pennoyer v. Neff*, 95 U.S. 714 (1877). Edward Q. Keasbey observed in 1905 that the English courts "of recent years have made an important departure" from the traditional rule that focused on service of process. Edward Q. Keasbey, *Jurisdiction over Non-Residents in Personal Actions*, 5 COLUM. L. REV. 436, 440 (1905).

[330] Norwich Pharmacal Co. v. Customs and Excise Comm'rs [1974] AC 133 (HL) (appeal taken from Eng.).

licensees in England found that their patent was infringed by the illicit importation of goods manufactured abroad.[331] However, they did not know who imported the illicit goods. They sought an injunction to the Commissioners of Customs and Excise for disclosure of the information. It was in this context that the House of Lords recognized this unusual doctrine of equity:

> . . . if through no fault of his own a person gets mixed up in the tortious acts of others so as to facilitate their wrong-doing he may incur no personal liability but he comes under a duty to assist the person who has been wronged by giving him full information and disclosing the identity of the wrongdoers.[332]

In the Age of the internet, this doctrine was quickly incorporated into English cyberlaw. A direct application of the *Norwich Pharmacal* doctrine is to seek an order on the ISP for information.[333] In 2011, the English High Court applied the doctrine to copyright protection by issuing an injunction order on British Telecommunications Plc.,[334] the largest internet service provider (ISP) in the U.K., to block certain websites that had infringed upon copyrights. In 2018, the United Kingdom Supreme Court brought the same doctrine to the area of trademarks.[335] Here, Swiss and German companies who owned luxury goods trademarks such as Cartier sought and obtained an injunction order from English courts against the UK's five largest ISPs for the purpose of blocking certain websites that were selling counterfeits.[336] In all these cases, ISPs, as the innocent third-party, have become the vehicle for enforcing intellectual property rights.

With the ISPs frequently being dragged to courts, the second barrier became less of a challenge. In September 2017, the New South Wales Supreme Court in Australia issued a worldwide injunction order on Twitter.[337] In a more significant case in Canada, Equustek Solutions Inc.,

---

[331] *Id.* at 137.

[332] *Id.* at 175.

[333] Golden Eye (Int'l) Ltd. v. Telefonica UK Ltd. [2012] EWCH (Ch) 723, [2012] RPC 698 (Eng.); Golden Eye (Int'l) Ltd. v. Telefonica UK Ltd. [2012] EWCA (Civ) 1740, [2013] RPC 452 (appeal taken from Eng.).

[334] Twentieth Century Fox Film Corp. v. British Telecomms. Plc. [2011] EWCH (Ch) 1981, [2012] All ER 806 (Eng.); Twentieth Century Fox Film Corp. v. British Telecomms. Plc. [2011] EWCH (Ch) 2714, [2012] All ER 869 (Eng.).

[335] Cartier Int'l AG v. British Telecomms. Plc. [2018] UKSC 28, [2018] 1 WLR 3259 (appeal taken from Eng.).

[336] *Id.*

[337] *X v Twitter, Inc* (2017) 95 NSWLR 301 (Austl.). For comments of the case, *see* Michael Douglas, *Extraterritorial Injunctions Affecting the Internet*, 12 J. EQUITY 34 (2018).

a British Columbia corporation, brought suit against Google Inc. and Google Canada.[338] The case began as a suit against a different company, Datalink, for infringement of trade secrets, and Equustek obtained numerous court orders, including a December 2012 order prohibiting Datalink from carrying business through any website.[339] However, Datalink continued selling the products in question in violation of court orders.[340] Following the December 2012 court order, Google, who was not a party to the dispute, voluntarily complied with the plaintiff's request to remove specific webpages or uniform resource locations ("URLs") from its Google.ca search results.[341] However, Google was unwilling to block an entire category of URLs ("mother sites") from its search results worldwide.[342] Equustek sought a worldwide interim injunction order against Google, a non-party to its case against Datalink.[343] In June 2014, the trial court ruled in favor of Equustek and granted an interim injunction.[344] The ruling was affirmed in July 2014 by the Court of Appeal of British Columbia.[345] In December 2017, the Canadian Supreme Court, by a majority of seven to two, dismissed the appeal and upheld the worldwide interlocutory injunction against Google.[346]

Emphasizing that interlocutory injunction is an equitable remedy, and thus a matter of discretion for the trial court,[347] the Supreme Court of Canada followed a three-part test in analyzing the question, asking: first, whether there is a serious issue to be tried; second, would the person applying for the injunction suffer irreparable harm if the injunction were not granted; and third, whether the balance of convenience favors granting the injunction or denying it.[348] The first part was not in dispute.[349] On the second part, Google did not dispute that Equustek may suffer irreparable harm but contended that a non-party should be immune from the

---

[338] Google Inc. v. Equustek Sols. Inc., 2017 SCC 34, [2017] 1 S.C.R. 824 (Can.).
[339] Equustek Sols. Inc. v. Jack, 2014 BCSC 1063 (Can.) (B.C.).
[340] *Id.* para 7.
[341] *Id.* para 9.
[342] *Id.*
[343] *Id.* para. 10.
[344] *Id.* para. 161.
[345] Equustek Sols. Inc. v. Google Inc., 2014 BCCA 295 (Can.) (B.C.); Equustek Sols. Inc. v. Google Inc., 2014 BCCA 448 (Can.) (B.C.); Equustek Sols. Inc. v. Jack, 2015 BCCA 265 (Can.).
[346] Google Inc. v. Equustek Sols. Inc., 2017 SCC 34, [2017] 1 S.C.R. 824 (Can.).
[347] *Id.* para. 23.
[348] RJR-MacDonald Inc. v. Canada (Attorney General), [1994] 1 S.C.R. 311, para. 40 (Can.).
[349] Google Inc. v. Equustek Sols. Inc., 2017 SCC 34, para. 26, [2017] 1 S.C.R. 824 (Can.).

injunction.[350] Here, the majority's answer was rather simple: Google's claim is "contrary to the jurisprudence."[351] The majority cited case law to clarify that "[t]he non-party's obligation arises 'not because [it] is bound by the injunction by being a party to the cause, but because [it] is conducting [itself] so as to obstruct the course of justice.'"[352] The majority declared, "where a non-party violates a court order, there is a principled basis for treating the non-party as if it had been bound by the order."[353] This is out of pragmatism, as "the interlocutory injunction in this case flows from the necessity of Google's assistance in order to prevent the facilitation of Datalink's ability to defy court orders and do irreparable harm to Equustek. Without the injunctive relief, it was clear that Google would continue to facilitate that ongoing harm."[354]

To the third part, the balance of convenience, Google contended that the global reach of the injunctive relief violates international comity.[355] The majority considered this only "theoretical."[356] Here, the Supreme Court quoted and fully endorsed what Madam Justice Fenlon, the trial judge, stated in her opinion: "most countries will likely recognize intellectual property rights and view the selling of pirated products as a legal wrong."[357] It also quoted, and fully endorsed, Justice Groberman of the Court of Appeal when the latter stated: "In the case before us, there is no realistic assertion that the judge's order will offend the sensibilities of any other nation."[358] In addition, the majority also noted that,

> [t]he order does not require that Google take any steps around the world, it requires it to take steps only where its search engine is controlled. This is something Google has acknowledged it can do—and does—with relative ease. There is therefore no harm to Google which can be placed on its 'inconvenience' scale arising from the global reach of the order.[359]

Two of the nine justices on the Supreme Court of Canada dissented.[360] The dissenting justices called for judicial restraint. From the viewpoint of ISP

---

[350] *Id.* paras. 26–27.
[351] *Id.* para. 28.
[352] *Id.* para. 29 (citing MacMillan Bloedel Ltd. v. Simpson, [1996] 2 S.C.R. 1048 (Can.)).
[353] *Id.* para. 29.
[354] *Id.* para. 35.
[355] *Id.* para. 44.
[356] *Id.*
[357] *Id.* para. 44 (quoting Equustek Sols. Inc. v. Jack, 2014 BCSC 1063, para. 144 (Can.)).
[358] *Id.* para. 45 (quoting Equustek Sols. Inc. v. Jack, 2015 BCSC 265, para. 93 (Can.)).
[359] *Id.* para. 43.
[360] *Id.* paras. 55–82 (Cote and Rowe, JJ., dissenting).

liability, two points they made are important to understand the majority's position as well as anticipate the next move of the Court. First, the dissenting justices continued Google's non-party claim and went further: "In our view, Google did not aid or abet the doing of the prohibited act."[361] This is because, the dissenting opinion continued, "[t]he act prohibited by the December 2012 Order is Datalink 'carrying on business through any website.' That act occurs whenever Datalink launches websites to carry out business—not when other parties, such as Google, make it known that such websites exist."[362] Therefore, the dissenting opinion concluded that "Google does not play a role in Datalink's breach of the December 2012 Order."[363]

Second, the dissenting justices noted that an alternative remedy was suggested by the Court of Appeal for British Columbia but was not considered by the majority.[364] The lower court suggested Equustek pursue a remedy in French court since Datalink has assets in France. "We see no reason why Equustek cannot do what the Court of Appeal urged it to do."[365]

In sum, courts in the Commonwealth countries responded to the internet by embracing and expanding the *Norwich Pharmacal* doctrine. This was based on the judicial power in equity, a common law tradition not foreign to the United States. However, in the United States, Section 230—a federal statute—and other policy considerations precluded that common law option.

B. EUROPEAN UNION

In the European Union, the Court of Justice of the European Union (CJEU) embraced the *Equustek* position, through its interpretation of the EU law. Article 15(1) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 provides guidance on certain legal

---

[361] *Id.* para. 71.

[362] *Id.* para. 69.

[363] *Id.* para. 74.

[364] *Id.* para. 81.

[365] *Id.* para. 81. For commentaries of the case, *see* Robert Diab, *Search Engines and Global Takedown Orders* Google v Equustek *and the Future of Free Speech Online*, 56 OSGOODE HALL L. J. 231 (Winter 2019); Douglas, *supra* note 337.

aspects of information society services, in particular electronic commerce, in the internal market.[366] Article 15(1) of that directive provides:

> Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

In *Glawischnig-Piesczek v. Facebook*,[367] the CJEU ruled in a defamation case complained by Eva Glawischnig-Piesczek, an Austrian citizen, a member of the Nationalrat (National Council, Austria), chair of the parliamentary party ("the Green"), and spokesperson for that party. On April 3, 2016, a Facebook user posted an article from an Austrian online news magazine *oe24.at* accompanied by a comment, both considered offensive and defamatory by Glawischnig-Piesczek.[368] On July 7, 2016, Glawischnig-Piesczek sent a letter to Facebook Ireland requesting the content be removed. Facebook did not remove the comment.[369] On December 7, 2016, Glawischnig-Piesczek brought an action before the Handelsgericht Wien (Commercial Court, Vienna, Austria).[370] The trial court in Vienna issued an interim order, directing Facebook Ireland to cease and desist from publishing and/or disseminating the offensive content.[371] Facebook Ireland complied with the order and blocked access to the content in Austria.[372] However, litigation continued, and eventually, the case was appealed to Oberster Gerichtshof (Supreme Court of Austria). Because the case raised questions on EU law, the Supreme Court of Austria referred it to the CJEU for a preliminary ruling on one question in particular: whether an EU member can issue a worldwide injunction order to remove the defamatory content.[373]

The CJEU held that "Directive 2000/31 does not preclude those injunction measures from producing effects worldwide."[374] The CJEU

---

[366] Directive 2000/31, of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1, 13.

[367] Case C-18/18, Glawischnig-Piesczek v. Facebook Ireland, Ltd., ECLI:EU:C:2019:821, (Oct. 3, 2019).

[368] *Id.* ¶ 12.

[369] *Id.* ¶ 14.

[370] *Id.*

[371] *Id.*

[372] *Id.* ¶ 15.

[373] *Id.* ¶ 20.

[374] *Id.* ¶ 50.

considered that "in view of the global dimension of electronic commerce, the EU legislature considered it necessary to ensure that EU rules in that area are consistent with the rules applicable at international level."[375] However, according to the CJEU, "[i]t is up to Member States to ensure that the measures which they adopt and which produce effects worldwide take due account of those rules."[376]

In sum, the CJEU concluded in *Glawischnig-Piesczek v. Facebook* that EU law is open to the idea of global injunction, similar to the Commonwealth countries.[377] It is interesting to note that, in *Google v. CNIL*,[378] the "right to be forgotten" case which was decided one week earlier, the CJEU concluded that the EU General Data Protection Regulation (GDPR) did *not* require the "right to be forgotten" to be enforced worldwide.[379] The different conclusions in the two cases likely show that the CJEU carefully meted out its decision and left this position open.

C. JAPAN

In Japan, the Provider Liability Limitation Act (PLLA) allows a victim whose rights are infringed upon to apply for an order issued to the service provider to release the content sender's name, address, and other information prescribed by the Ministry of Internal Affairs and Communications.[380] In May 2002, the Ministry issued an ordinance providing a list of information that may be disclosed under Article 4(1),[381] including, name, address, email, IP address, mobile phone number, etc. With the rise of social concerns with online defamation in Japan, Article 4(1) offers a possible pathway for aggravated parties to seek disclosure of

---

[375] *Id.* ¶ 51.

[376] *Id.* ¶ 52.

[377] *Id.*

[378] Case C-507/17, Google v. CNIL, ECLI:EU:C:2019:772, ¶¶ 63–64 (Sept. 24, 2019).

[379] *Id.* ¶ 65.

[380] PROVIDER LIABILITY LIMITATION ACT art. 4(1) (Japan). For a summary in English, *see* MASAO YANAGA, *supra* note 298, at 199.

[381] Tokutei Denki Tsūshin Ekimu Teikyōsha No Songai Baishō Sekinin No Seigen Oyobi Hasshinsha Jōhō No Kaiji Nikansuru Hōritsu Dai Yon Jō Dai Ichi Kō No Hasshinsha Jōhō O Sadameru Shōrei (特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律第四条第一項の発信者情報を定める省令) [Ministry Ordinance Based on Article 4(1) of Provider Liability Limitation Act], Law No. 57 of 2002, (e-Gov Hōrei kensaku [Hōrei DB]), https://elaws.e-gov.go.jp/document?lawid=414M60000008057 [https://perma.cc/SC9E-6VBH] (Japan).

information of the wrongdoers from ISPs in order to obtain remedy.[382] So far, the Supreme Court of Japan (SCJ) has made three decisions on Article 4(1). The first decision was in April 2010, when the SCJ ruled that the ISP was the one who had the duty to disclose under Article 4(1).[383] The second case was decided one week later, when the SCJ ruled that ISP would be liable for compensation for its failure to disclose.[384] The third case was decided by SCJ in July 2020 in a copyright dispute against Twitter,[385] the American corporation based in Silicon Valley, California.

The plaintiff in *Twitter* was a copyright owner of a photograph, with a copyright mark and his name; he posted the photograph on his website in 2009.[386] In 2015, without permission, a Twitter user copied the photograph and used it in his or her tweet.[387] The photograph was retweeted many times by other Twitter users.[388] When retweeted, Twitter automatically resized the photos, so the copyright mark and owner's name disappeared from the retweeted photos.[389] The SCJ concluded that this omission of the owner's name infringed upon the owner's moral rights

---

[382] Japan maintains criminal libel law, and traditionally, criminal law was and still is frequently used to deal with defamation cases. For example, Lawrence W. Beer observed in 1972, "As a matter of doctrine, civil suit is the preferred remedy, except in extreme cases. However, in practice criminal prosecution or recourse to the Civil Liberties Bureau are the usual avenues in Japan." Lawrence W. Beer, *Defamation, Privacy, and Freedom of Expression in Japan*, 5 LAW IN JAPAN 192 (1972). This observation is even truer in the age of the internet. Professor Salil K. Mehra showed that criminal libel law use increased from 1994 to 2003, when the use of internet in Japan skyrocketed. Salil K. Mehra, *Post a Message and Go to Jail Criminalizing Internet Libel in Japan and the United States*, 78 U. COLO. L. REV. 767 (2007). Recently, the Ministry of Justice has advocated introducing more severe criminal penalties for the crime of insults (侮辱罪). *See* 侮辱罪に懲役刑導入へ [Imprisonment to be Introduced for Insult Crimes], 日本経済新聞 [JAPANESE ECON. NEWS], Aug. 31, 2021, at 44. Civil remedy in defamation cases remains limited by American standards. *See* Noriko Kitajima, *The Protection of Reputation in Japan A Systemic Analysis of Defamation Cases*, 37 LAW & SOC. INQUIRY 89 (Winter 2012). In this sense, Article 4(1) of PLLA is a step forward in strengthening civil remedies in Japan.

[383] Saikōsaibansho Daiichishō Hōtei [Supreme Court First Small Court] Apr. 8, 2010, Heisei 21 (kyo) No. 3, 64 SAIKŌ SAIBANSHO MINJI HANREISHŪ [MINSHŪ] 676, (Japan), available at https://www.courts.go.jp/app/hanrei_jp/detail2?id=80093 [https://perma.cc/PNV2-EFYA]. For a summary in English, see MASAO YANAGA, *supra* note 298, at 199.

[384] Saikōsaibansho Daisanshō Hōtei [Supreme Court Third Small Court] Apr. 13, 2010, Heisei 21 (kyo) no. 3, 64 SAIKŌ SAIBANSHO MINJI HANREISHŪ [MINSHU] 758, available at https://www.courts.go.jp/app/hanrei_jp/detail2?id=80104 [https://perma.cc/N7QT-4TBH].

[385] Saikō Saibansho [Supreme Court] July 21, 2020, 2018 (Ju) 1412 no. 4, 74 SAIKŌ SAIBANSHO MINJI HANREISHŪ [MINSHU], available at https://www.courts.go.jp/app/hanrei_en/detail?id=1776 [https://perma.cc/H3TR-JDVH] [hereinafter *Twitter* case].

[386] *Twitter* case, supra note 385.

[387] *Id.*

[388] *Id.*

[389] *Id.*

under the Copyright Act.[390] Therefore, under PLLA Article 4(1), the Court affirmed the trial court's order to Twitter to disclose the identification information of the user who has sent the initial tweet.[391]

The *Twitter* ruling, explosive as it was,[392] was narrowly formulated. The SCJ was largely focused on the statutory language of PLLA Article 4(1) and the Copyright Act,[393] which is typical of the SCJ. If the SCJ was concerned about policy issues, it is more likely that it was driven by growing domestic concerns of defamation in cyberspace. Since the SCJ's 2010 decisions, online abuse (ネット中傷, *netto chōshō*) has been increasingly considered a serious social concern in Japan.[394] In July 2011, the Ministry of Internal Affairs and Communications publicized a study of PLLA with suggestions.[395] In November 2013, the Japan Federation of Bar Associations called for reform of PLLA.[396] In February 2020, the Cabinet proposed, and the Diet (Japan's bicameral legislature) passed a new law, the "Digital Platform Transparency Act."[397] Shortly before the SCJ's decision, in May 2020, Hana Kimura (木村花), an actress on a popular reality TV show, died of suicide after receiving countless hostile online

---

[390] *Id.*

[391] *Id.*

[392] Shunsuke Abe, Shashin No Mudan Tōkō , Ritsuīto Dake Demo Kenri Shingai Saikōsai (写真の無断投稿、リツイートだけでも権利侵害 最高裁) [*The Supreme Court Says Using Photos Without Permission, Even Retweets, Is Infringement of Copyrights*], ASAHI SHINBUN (朝日新聞) [Asahi Shimbun Digital] (July 21, 2020, 6:28 PM), https://www.asahi.com/articles/ASN7P5CN2N7KUTIL02G.html [https://perma.cc/HQ7T-E387].

[393] Only Justice Keiichi Hayashi's sole dissenting opinion noted the policy issue—the burden imposed on the 45 million Twitter users in Japan. *Twitter* case, *supra* note 385.

[394] 安保克也 [Katsuya Anbo], インターネット上における名誉毀損 [*Defamation on the Internet Domestic Cases in Japan*], 6 日本国際情報学会誌 [JOURNAL OF JAPANESE SOCIETY FOR GLOBAL AND CULTURAL STUDIES] 39 (2009) (discussing online abuse as a broad social issue in Japan).

[395] Purobaida Sekinin Seigenhō Kenshō Nikansuru Teigen (プロバイダ責任制限法検証に関する提言) [Proposals for Examining the Provider Liability Limitation Act], Sōmushō (総務省) [Ministry of Internal Affairs and Communications], (July 21, 2011), https://www.soumu.go.jp/menu_news/s-news/01kiban08_01000037.html [https://perma.cc/J55L-J3L6].

[396] Nippon Bengoshi Rengōkai (日本弁護士連合会) [Japan Federation of Bar Associations], Purobaida Sekinin Seigenhō Kaisei Nitsuite No Yōbōsho (プロバイダ責任制限法改正についての要望書) [What We Hope for in Reforming the Provider Liability Limitation Act] (Nov. 6, 2013), https://www.nichibenren.or.jp/document/opinion/year/2013/131106.html [https://perma.cc/94LL-W9SA].

[397] Keizai Sangyōshō (経済産業省) [Ministry of Economy, Trade and Industry], Tokutei Dejitaru Purattofōmu No Tōmeisei Oyobi Kōseisei No Kōjō Nikansuru Hōritsuan Ga Kakugi Kette Saremashita (「特定デジタルプラットフォームの透明性及び公正性の向上に関する法律案」が閣議決定されました) [Cabinet Decided on "Improving Specific Digital Platform Transparency and Fairness Bill"] (Feb. 18, 2020), https://www.meti.go.jp/press/2019/02/20200218001/20200218001.html [https://perma.cc/RC4M-V9JC].

messages.[398] The Kimura tragedy became a powerful signal showing how serious the problem of online abuse was. But concerns of the online world were not limited to Japan's territory. In June 2020, the Diet passed extensive amendments to the Act on Protection of Personal Information (APPI).[399] One significant change in the 2020 amendments is that APPI is now applicable inside as well as outside Japan's territory.[400] In this context, the SCJ's ruling in *Twitter*, by affirming a trial court's order to an American corporation based in California, seems to suggest an emerging policy shift in Japan. At least, the SCJ puts itself in a potential position like that of the Canadian Supreme Court in asserting global jurisdiction.

D. CHINA

China's judiciary has not issued any global injunction orders in online cases as of November 2021. Traditionally, it has been constrained by its own ideological and political factors. However, in recent years, China's policymakers have reconsidered their position. This new direction is indicated in a speech given by President Xi Jinping on February 25, 2019, where the President called on efforts to further "extraterritorial application" (*yuwai shiyong*, 域外适用) of Chinese law.[401]

Leading scholars in China largely frame President Xi's new direction with the reform of the Civil Procedure Code, especially on the question of international jurisdiction of the Chinese courts. The Civil

---

[398] "Terasu Hausu" Shutsuen Chū No Joshi Puroresurā Shikyo 22 Sai (「テラスハウス」出演中の女子プロレスラー死去 22歳) [Girl in "Terrace House" Show Who Played Professional Wrestler, Died at 22], 朝日新聞 [ASAHI SHIMBUN DIGITAL] (May 23, 2020), https://www.asahi.com/articles/ASN5R5GF6N5RUCVL006.html [https://perma.cc/T4GB-38AQ].

[399] 個人情報の保護に関する法律等の一部を改正する法律 [Amendments to the Act on Protection of Personal Information], passed at the Diet of Japan on June 5, 2020, promulgated on June 12, 2020, available at https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/#gaiyo [https://perma.cc/8QWQ-GW7D] [hereinafter APPI 2020 Amendment] (last accessed Aug. 20, 2021).

[400] *Id.* For comments, *see* Akeshige Sugimoto, Akihiro Kawashima & Tobyn Aaron, *A New Era for Japanese Data Protection 2020 Amendments to the APPI* (Apr. 13, 2021), https://fpf.org/blog/a-new-era-for-japanese-data-protection-2020-amendments-to-the-appi/#:~:text=The%202020%20Amendments'%20broadened%20extraterritorial,and%20to%20implement%20any%20necessary [https://perma.cc/P5EU-P9R7] (last accessed Aug. 20, 2021).

[401] Xi Jinping Zhuchi Zhaokai Zhongyang Quanmian Yifa Zhiguo Weiyuanhui Di Er Ci Huiyi Bing Fabiao Zhongyao Jianghua (习近平主持召开中央全 依法治国委员会第二次会议并发表重要讲话) [*Xi Jinping Opens the Second Meeting of the Party Central Commission on Rule by Law and Delivers Keynote Speech*] (Feb. 25, 2019, 8:15 PM), http://www.gov.cn/xinwen/2019-02/25/content_5368422.htm [https://perma.cc/8X86-U2XQ].

Procedure Code, last amended in 2012,[402] was based on an outdated and conservative notion of territorial focus that has failed to notice China's changed circumstances, including China's new status as a capital-exporting country with foreign investments all over the world. For others, this is more than a practical concern of China's interests overseas, it is also about China being a "great power" (*daguo*, 大国); thus, it should meet the expectations of the "judiciary of a great power" (*daguo sifa*, 大国司法).[403] That means that China should be able to project judicial power outside its own territory. The pressure China felt in the cases of Huawei, ZTE, and the arrest of Meng Wanzhou, Huawei's chief financial officer, prompted intense interest in long-arm statutes in the United States.[404] The other factor is China's "Belt and Road Initiative" (BRI), where China feels the need to reach all countries at the receiving end of the BRI investments. Think tanks and scholars are suggesting that China should have its own long-arm statute.[405]

So far, the most significant development of this "extraterritorial application" of Chinese law policy is unmistakably manifested in the newly enacted Data Security Law (DSL).[406] Paragraph 2 of the Article 2 of the DSL prescribes: "Data handling activities carried out outside the Chinese territory of the P.R.C. that harming the national security of the P.R.C., the public interest, or the lawful rights and interests of citizens and organizations, are to be pursued for legal responsibility in accordance with law."[407] According to the explanatory statement made to the National People's Congress Standing Committee when the draft law was submitted

---

[402] *E.g.*, Li Wang (李旺), Guoji Minshi Caipan Guanxia Quan Zhidu Xi—Jian Lun 2012 Nian Xiugai de "Minshi Susong Fa" Guanyu Shewai Minshi Anjian Guanxia Quan de Guiding (国际民事裁判管辖权制度析—兼论 2012 年修改的《民事诉讼法》关于涉外民事案件管辖权的规定) [*An Analysis of International Civil Jurisdiction—with a Comment on the Foreign Related Civil Jurisdiction Rules in the 2012 Revised Civil Procedure Code*], Guojifa Yanjiu (国际法研究) [STUDIES OF INTERNATIONAL LAW] 89 (2014).

[403] He Qisheng (何其生), Daguo Sifa Linian Yu Zhongguo Guoji Minshi Susong Zhidu de Fa Zhan (大国司法理念与中国国际民事诉讼制度的发展) [*The Judiciary of a Great Power and the Development of China's Civil Procedure in International Cases*], Zhongguo Shehui Kexue (中国社会科学) [SOCIAL SCIENCES IN CHINA] 123 (2017).

[404] *See* Xiao Yongping (肖永平), Chang bi Guanxia Quan de Fali Fenxi Yu Duice Yanjiu ("长臂管辖权"的法理分析与对策研究) [*A Jurisprudential Analysis of the "Long-arm Jurisdiction" and Responses*], Zhongguo Faxue (中国法学) [LEGAL SCIENCE IN CHINA] 39 (2019).

[405] Frank Tang, *China Urged to Flex Long-Arm Jurisdiction to Protect Its Companies from Foreign Hostility*, SOUTH CHINA MORNING POST (Sept. 17, 2020, 6:00 AM), para. 1, https://www.scmp.com/economy/china-economy/article/3101803/china-urged-flex-long-arm-jurisdiction-protect-its-companies [https://perma.cc/ZB7S-2TB5].

[406] Data Security Law of the People's Republic of China, *supra* note 6.

[407] *Id.* art. 2.

for a vote, extraterritorial application was a considered "necessary" in order to fully protect data security.[408] Similarly, Article 3 of the newly enacted Personal Information Protection Law (PIPL 2021) prescribes:

> This law is also applicable to activities outside the PRC territory that process the personal information of natural persons within the territory of the PRC, in any of the following circumstances:
>
> (1) for the purpose of providing products or services to natural persons within the territory;
>
> (2) to analyze and evaluate the conduct of natural persons in the territory;
>
> (3) Other circumstances provided for by laws and administrative regulations.[409]

The language in both statutes is general and ambiguous, aiming to serve both ideological function as well as legislative one. It sends a clear enough message to the Chinese judiciary. Chinese courts may not make any decision like *Equustek* immediately, but there is no question that policy is pointing in that direction.

V. CONCLUSION

In cyberspace, an unprecedented judicial divergence is happening. In the United States, the global center of the internet and the home of many major digital platforms, jurisprudence is based on a globalization characterized by self-regulation, which is in line with American commercial interests and First Amendment ideology. On the other side, however, is the courts in Commonwealth countries, the European Union, and Japan—whose policy is characterized by a public regulation approach—who are increasingly more assertive in claiming jurisdiction, applying tort-based standards, and more open to global enforcement against global digital platforms. Anxious of losing their own competitive edge, even the very control of their economy and social values in the digital era, these countries consider "surveillance capitalism" more of an

---

[408] Liu Junchen (刘俊臣), Guanyu "Zhonghua Renmin Gongheguo Shuju Anquan Fa (Cao'an) de Shuoming (关于《中华人民共和国数据安全法（草案）》的说明) [*An Explanatory Statement on the Draft Digital Data Security Law of the People's Republic of China*], Zhong Hua Renmin Gongheguo Quanguo Renmin Daibiao Dahui Changwu Weiyuanhui Gongbao (中华人民共和国全国人民代表大会常务委员会公报) [GAZETTE OF THE STANDING COMMITTEE OF THE NATIONAL PEOPLE'S CONGRESS OF THE PEOPLE'S REPUBLIC OF CHINA] 956 (2020).

[409] Personal Information Protection Law of the People's Republic of China, *supra* note 6, art. 3.

American problem that must be addressed by a revolt against the American regulatory approach. This is also true in the third camp—China. From the very beginning, China was driven by its own ideology and self-interests, but it had the same need to assert control of the internet. In cyberspace, China's regulatory approach has double targets: American platforms as well as China's homemade surveillance capitalism—China's digital platforms, which all started as non-state corporations. For this goal, China borrows ideas and conceptual tools from the second camp in building its own regulatory apparatus. The result of these developments in both the second and third camps is a widening judicial divergence that belies an underlying revolt against US hegemony—the "Brussels' effect" on a global scale.[410]

For convergence believers—the generations of American globalists and comparative lawyers who confidently believe that the United States is a model for the rest of the world—this is a shocking development. A global revolt is different from a claim that the American model is less appealing;[411] it is a claim that judges and lawmakers in all of America's major trading partners are consciously embracing a different regulatory approach in response to American refusal to regulate their digital platforms at home. From the vantage point of 2021, this divergence may well be a new normal stuck with us for some time. Recently in the United States, while there are some measures taken on the state level[412] or on the federal level by the Biden Administration,[413] it is hard to anticipate in the short term any significant change like that of the EU's proposed bills such as the Digital Markets Act and the Digital Services Act.[414]

---

[410] Bradford, *supra* note 33, at 3.

[411] *See* David S. Law & Mila Versteeg, *The Declining Influence of the United States Constitution*, 87 N.Y.U. L. REV. 762, 767 (2012).

[412] On July 7, 2021, Colorado enacted the Comprehensive Data Privacy Act (SB 21-190) (CCDPA), making Colorado the third state on such privacy law in the United States. *See* Colorado Privacy Act, ch. 483, 2021 Colo. Sess. Laws 3445. Virginia was the second state to enact Consumer Data Protection Act (VCDPA), on March 2, 2021. *See* Consumer Data Protection Act, ch. 35, 2021 Va. Acts. Both CCDPA and VCDPA will go into effect on January 1, 2023. The first state was California, with the Consumer Privacy Act of 2018 (CCPA) and the California Privacy Rights Act of 2020 (CPRA). National Conference of State Legislatures, *2020 Consumer Data Privacy Legislation* (Jan. 17, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx [https://perma.cc/93K7-UBMP].

[413] Brent Kendall, *New U.S. Antitrust Suit Targets Facebook*, WALL ST. J., Aug. 20, 2021, at A2. *See also supra* note 23.

[414] Digital Services Act, *supra* note 10; Digital Markets Act, *supra* note 10.

This state of regulatory divergence in cyberspace, however, not only fragments the internet but also cancels out the supposed "benefits" of self-regulating at-home. This is particularly important as major digital platforms have more users in foreign markets and derive more revenue overseas. [415] American policymakers, should they find themselves increasingly in a political predicament, are not alone. The global digital platforms are trapped in an awkward situation too, though a slightly different one. While they are often out of the reach of courts or are protected by Section 230 immunity at home, they prove to themselves and the world that they are capable of being more responsive and accountable to their users in foreign markets when required by local law and enforced by local courts. Whatever they tell Congress or the general public to justify the status quo, they know they are acting in bad faith.

---

[415] In the year 2020, for example, Facebook had more users in foreign markets and more revenue from foreign markets. *See* Mansoor Iqbal, *Facebook Revenue and Usage Statistics (2021)*, BUS. OF APPS, (Sept. 24, 2021) https://www.businessofapps.com/data/facebook-statistics/ [https://perma.cc/V3RP-J4MJ].