CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission on Internet Governance

ourinternet.org

PAPER SERIES: NO. 42 — NOVEMBER 2016

Internet Intermediaries as Platforms for Expression and Innovation

Anupam Chander

INTERNET INTERMEDIARIES AS PLATFORMS FOR EXPRESSION AND INNOVATION

Anupam Chander

Published by the Centre for International Governance Innovation and Chatham House.

This work was carried out with the aid of a grant from the International Development Research Centre (IDRC), Ottawa, Canada.

The views expressed herein do not necessarily represent those of IDRC or its Board of Governors.

67 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

TABLE OF CONTENTS

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

Launched by two independent global think tanks, the Centre for International Governance Innovation (CIGI) and Chatham House, the Global Commission on Internet Governance will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

The Global Commission on Internet Governance will focus on four key themes:

- enhancing governance legitimacy — including regulatory approaches and standards;
- stimulating economic innovation and growth — including critical Internet resources, infrastructure and competition policy;
- ensuring human rights online — including establishing the principle of technological neutrality for human rights, privacy and free expression; and
- avoiding systemic risk — including establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence-building measures and disarmament issues.

The goal of the Global Commission on Internet Governance is two-fold. First, it will encourage globally inclusive public discussions on the future of Internet governance. Second, through its comprehensive policy-oriented report, and the subsequent promotion of this final report, the Global Commission on Internet Governance will communicate its findings with senior stakeholders at key Internet governance events.

www.ourinternet.org

ABOUT THE AUTHOR

Anupam Chander is Martin Luther King, Jr. Professor of Law and director of the California International Law Center at the University of California, Davis. A graduate of Harvard College and Yale Law School, Anupam has been a visiting professor at Yale, Chicago, Stanford and Cornell. He is the author of *The Electronic Silk Road: How the Web Binds the World Together in Commerce* (Yale University Press). He practised law in New York and Hong Kong with Cleary, Gottlieb, Steen & Hamilton. He served on the executive council of the American Society of International Law and serves as a judge for the Stanford Junior International Faculty Forum. The recipient of Google Research Awards and an Andrew Mellon grant on the topic of surveillance, Anupam has served as a member of the International Centre for Trade and Sustainable Development and the World Economic Forum expert group on the digital economy.

EXECUTIVE SUMMARY

Because they stand at the crossroads of commerce, society and even politics, Internet intermediaries increasingly draw the attention of national governments seeking to regulate what occurs within their borders. Frustrated with trying to control the multitudinous individuals empowered by a global Internet, governments often see online intermediaries as a route to online control. Governments seek to utilize Internet intermediaries as both censors and police, urging them to take down online information that governments dislike and to hand over information that governments want.

But the imposition of the role as censor and police for the Information Age undermines the individual empowerment that online intermediaries can provide. Making online intermediaries liable for the information exchanged on their platforms leads the intermediaries to shutter even permissible speech, lest they face ruinous damage claims. Making online intermediaries act as police informants leads individuals to censor themselves, lest the individuals draw unwanted attention from the authorities or the intermediaries.

Requirements to monitor content for fear of liability not only undermine speech and liberty, but they also deter innovation. Liability for the actions of one's users can make the provision of a service uneconomical.

The challenge is to encourage Internet intermediaries to help people find what they are looking for, share with each other what they want to share, and educate themselves, in ways that are consistent with both local and international law.

INTRODUCTION[1]

Many of the biggest companies in the world today are intermediaries for online information. Facebook intermediates information sharing among its 1.5 billion users. Google intermediates the entire Internet for individuals performing more than three billion searches a day. Alibaba intermediates the distribution of wares from millions of sellers to 350 million buyers across the world in a single year. Tencent's WeChat app intermediates messages among some 700 million people. Individuals across the world upload 400 hours of video every minute to YouTube (Brouwer 2015). Internet companies serve as intermediaries for literally billions of transactions a day. They have become a crucial means for communication and commerce, as well as for education and entertainment. The Chinese website Qidian.com, to cite another example, is "the world's leading self-publishing platform, with 1 million registered writers and 100 million paying members" (Box and West 2016, 52).

For better or worse, Internet intermediaries have become a focal point for Internet regulation across the world. Because they help businesses, organizations and individuals to connect across the world in ever more domains of life, Internet intermediaries have come to be seen as crucial arbiters of what is allowed and not allowed in a society. Governments see Internet intermediaries as central points at which to exercise control, a far easier task than to regulate the individuals who use the Internet directly. Governments often require intermediaries to censor information so that it is not distributed among their citizenry, and also to turn over some of the information they gather from their users.

But requiring Internet intermediaries to serve as online censors and police harms free expression and undermines the development of new enterprises, which generally lack the resources to satisfy extensive monitoring obligations. When the law exposes intermediaries to liability for the actions of their users, intermediaries have an economic incentive to censor anything potentially controversial. When the law requires intermediaries to reveal the actions of their users to the police, individuals refrain from even legal actions.

Internet intermediaries can foster freedom online, or they can undermine it, through censoring and monitoring the population.

GLOBAL INTERMEDIARIES, LOCAL PROBLEMS

Intermediaries have long existed — think real-estate agents to stockbrokers to the village matchmaker. Yet, there is something different, both quantitatively and qualitatively, about the new breed of intermediaries on the Internet. The Internet has brought with it new types of intermediaries with new capabilities operating at scales far beyond yesteryear's librarians and brokers. These intermediaries now operate not at the scale of a town, but at the scale of a country or even the world. YouTube offers a local version in more than 88 countries, in 76 different languages; 80 percent of YouTube's views come from outside the United States,[2] where it is headquartered.

Online intermediaries include a wide array of companies essential to the Internet: Internet service providers (ISPs), which provide Internet access to households and businesses; Internet hosting services, which rent computer server space to others; social media platforms (in so-called

1 The author thanks Anna Barich for excellent research assistance, and is grateful for a Google Research Award supporting related research. Some of the passages herein are drawn from "How Law Made Silicon Valley" (Chander 2014a, 653–56, 670–72, 675-676), "Law and the Geography of Cyberspace" (Chander 2014b, 104-105) and "Free Speech" (Chander and Le 2014).

2 See www.youtube.com/yt/press/statistics.html.

Web 2.0 services), which allow users to share writing, photos, audio and video; and search engines. More recently, new forms of Internet intermediaries, such as Uber, Didi Chuxing and Airbnb, have arisen. Relying on the fact that smartphones know where we are at all times, these new intermediaries offer services tailored to an individual's precise location in the world. Thus, today's intermediaries depend on both the micro scale of the Internet, pinpointing where a user is geographically, and the macro scale of the Internet, allowing intermediaries to connect, quite literally, one billion people in a day.

Online intermediaries have increasingly found themselves part of global flashpoints concerning local regulation. Take a few recent examples. A Brazilian court has frozen US$6 million in a Facebook bank account in Brazil because Facebook says it cannot access or decrypt messages sent via its Whatsapp platform in a case involving illicit drugs (Reuters 2016a). Hungary now has a law permitting the national communications authority to block Internet access to "illegal dispatcher services" (Dunai 2016), thus granting the government the ability to ban intermediaries such as Uber and Didi Chuxing.

Since today's intermediaries often operate across national borders, connecting people wherever they may be, intermediaries are subject to rules that often vary or even conflict in what they allow or require.

FREE EXPRESSION

Article 19 of the United Nation's Universal Declaration of Human Rights states that freedom of expression is a universal human right: "Everyone has the right to freedom of opinion and expression; the right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media regardless of frontiers" (United Nations 1948). The civil society group Article 19, named after the provision, argues that intermediary liability rules can adversely affect freedom of expression. It observes "risks posed by the currently widespread regime of liability to the exercise of freedom of expression online" (Article 19 2013, 4). It accordingly proposes that "hosts should in principle be immune from liability for third-party content in circumstances where they have not been involved in modifying that content" (ibid., 16).

Online intermediaries have helped make the Internet the modern town hall and village square. There is an emerging consensus in the human rights community that limiting intermediary liability promotes freedom of expression. As a report for UNESCO by Internet freedom advocate Rebeccca MacKinnon and others concludes, "limiting the liability of intermediaries for content published or transmitted by third parties is essential to the flourishing of internet services that facilitate expression" (MacKinnon et al. 2014, 179). UN Special Rapporteur Frank LaRue (2011, 6-7) observed the value of Internet intermediaries to freedom of expression:

> With the advent of Web 2.0 services, or intermediary platforms that facilitate participatory information sharing and collaboration in the creation of content, individuals are no longer passive recipients, but also active publishers of information...platforms are particularly valuable in countries where there is no independent media, as they enable individuals to share critical views and to find objective information.

LaRue observed the simple logic that leads from intermediary liability to censorship: "Given that intermediaries may still be held financially or in some cases criminally liable if they do not remove content upon receipt of notification by users regarding unlawful content, they are inclined to err on the side of safety by overcensoring potentially" (ibid., 12). In their 2011 Joint Declaration on Freedom of Expression and the Internet, the four UN special rapporteurs on freedom of expression recommended that:

> No one who simply provides technical Internet services such as providing access, or searching for, or transmission or caching of information, should be liable for content generated by others, which is disseminated using those services, as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so ('mere conduit principle').…At a minimum, intermediaries should not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression (which is the case with many of the 'notice and takedown' rules currently being applied). (UN Special Rapporteur et al. 2011)

But online intermediaries have often been targeted precisely because of the information they help disseminate. In the wake of the horrendous attack on Istanbul's Ataturk Airport this year, Turkey's government reportedly moved to block or throttle (slow down) Facebook, Twitter and YouTube. An Istanbul court "later expanded the order to include all media, noting that news about the attack may spread 'fear and panic, which may serve to the intentions of terrorist groups'" (Risen 2016).

INTERMEDIARY LIABILITY LAW

The law regulating Internet intermediaries varies across the world. A comparison of legal regimes shows that the United States is notably more hospitable to such enterprises than many other leading technologically advanced nations.

What follows is a comparison of the intermediary liability laws of the United States and those of the European Union and Japan.

INTERMEDIARY LIABILITY LAW IN THE UNITED STATES

In the 1990s, the US Congress passed two pieces of legislation that proved essential to the rise of the global Internet as we know it today: the Communications Decency Act (CDA) of 1996 and the Digital Millennium Copyright Act (DMCA) of 1998. These statutes helped encourage the development of Internet intermediaries by increasing confidence that they would not be held liable if a user utilized their services to violate someone else's rights.

Because many (and perhaps most) individuals will infringe copyright at some point when they use online services to share information, holding the online service liable for that infringement would make that service leery of open-ended sharing. Perhaps a service would have to monitor each user post — an expensive proposition. Monitoring obligations would make impossible a service such as Craigslist, where individuals and businesses post some 80 million classified advertisements a month.[3] Each of Craigslist's 40 employees would have to review two million advertisements per month, or Craigslist would have to hire legions more employees, jeopardizing its ability to offer a free service supported by advertising alone.

Any technology that allows individuals to share information can lend itself to copyright infringement. A company like Yahoo that allows individuals to post whatever they want online faces a high risk that its service will be used for extensive copyright infringement. Such a company would be liable for direct infringement every time it delivered a copy of a copyrighted work, for contributory infringement if it had knowledge and made a material contribution to the infringement, and for vicarious infringement if it controlled and earned a direct financial benefit from the infringement. Given that statutory damages for direct infringement alone range from US$200 to US$150,000 per work,[4] and that millions of works are copied online each day, the spectre of liability would be enough to stop most Internet companies in their tracks.

The DMCA offered ISPs safe harbours from liability for copyright infringement by users. The DMCA established a notice-and-takedown regime that did not place the policing burden for discovering copyright infringement on the Internet intermediary. Rather than monitoring their own networks for possible copyright infringement — a costly and difficult task — online intermediaries could wait for copyright holders to notify them of specific infringements. The statute insulated Internet intermediaries that duly cooperated with copyright holders upon receiving a notice of infringement.[5] This had a clear effect: relying on the DMCA, US courts, for example, sided with YouTube against Viacom's claims that YouTube abetted copyright infringement by holding that YouTube could not be held liable for users who uploaded Viacom's copyrighted videos.[6]

The DMCA achieved a relatively peaceful coexistence between northern and southern California — where technology companies in Silicon Valley, in the north, would banish repeat offenders and take down material if requested by the copyright owners, often based in Hollywood, in the south. By performing these duties diligently, Silicon Valley enterprises generally managed to avoid liability for the widespread copyright infringement that still occurred through their systems. While some have legitimately criticized Title II (the Online Copyright Infringement Liability Limitation Act) of the DMCA for leading firms to take down material too quickly for fear of jeopardizing their safe harbour, the DMCA marked a significant accomplishment for Silicon Valley in creating rules that allowed Web 2.0 enterprises to flourish without either excessive copyright-management costs or high liability risks.

Section 230 of the CDA warded off claims for intermediary liability for defamation and a host of other civil claims. Again and again, Section 230 proved invaluable to shield web enterprises from lawsuits, as demonstrated by a plethora of cases.[7] Perhaps every major Internet enterprise has relied on the statute to defend itself over the years. CDA Section 230 insulated web enterprises from the reach of a variety of federal and state causes of action, both statutory and common law (Lemley 2007). These include, for example, the Federal Fair Housing Act, Title II of the Civil Rights Act of 1964, the Washington State Consumer Protection Act, and common law actions such as invasion of privacy, negligence and tortious interference with

3 See www.craigslist.org/about/factsheet.

4 Copyright Act, Title 17, US Code, Section 504(c)(1)-(2) (2012) (providing statutory damages of $750 to $30,000 per work, but permitting damages per work to be reduced to $200 in cases where the defendant was not aware, and had no reason to believe, that infringement was occurring, or increased to $150,000 in cases of willful infringement).

5 DMCA, Title 17, US Code, Section 512 (1998).

6 *Viacom Int'l Inc. v. YouTube Inc.* 940 F. Supp. 2d 110 (SDNY 2013); *Viacom Int'l Inc. v. YouTube Inc*. 676 F.3d 19 (2nd Cir. 2012).

7 For a lengthy list of examples, see Chander (2014a, 653–55, n58).

business relations. As the US Fourth Circuit Court of Appeals noted, a notice-and-takedown system would inevitably lead to firms generally choosing to take down controversial statements rather than face any spectre of liability.[8] As Neal Katyal (2001, 1007-1008) writes, "because an ISP derives little utility from providing access to a risky subscriber, a legal regime that places liability on an ISP for the acts of its subscribers will quickly lead the ISP to purge risky ones from its system."

Protection from liability has depended not only on congressional action, but also on judicial interpretation and common law-making. The DMCA's safe harbours for Internet intermediaries are limited to protections from copyright-infringement claims, and Section 230 of the CDA does not apply to intellectual property claims. Courts interpreting common law doctrines have acted on their own to limit the liability of online intermediaries for trademark infringement by users.

The end result was that, for more or less the same behaviour, an Internet company might find itself in legal trouble in Europe but scot-free in the United States. An entrepreneur founding a company that allows individuals across the world to buy and sell goods might well choose the United States as a more welcoming legal regime to register with. Such a company based in Europe might find itself encumbered by obligations to determine whether the multitude of goods sold on its site were authentic. Such a burden might well prove too demanding for a fledgling corporation. Consider the case of eBay. Two years after its founding, in 1995, eBay still had fewer than 50 employees. A year later, in mid-1998, with 76 employees, it was hosting 500,000 items for sale, with 70,000 items added per day. At the time, it was valued at US$2 billion. It is hard to imagine that such a small group of employees could have vetted the literally tens of thousands of classified items coming in each day to ascertain whether they were authentic (Chander 2014b, 104-105).

Despite popular understanding of the United States as an intellectual property maximalist state, US intellectual property law has proven a good deal more flexible than that in other technologically advanced states. The hospitable legal framework did more than help American enterprise, it has created what has become the engine for free speech across the world today. US companies now serve as free-expression platforms for the world.

INTERMEDIARY LIABILITY LAW IN THE EUROPEAN UNION

The European Union's intermediary liability law proved less welcoming to Internet entrepreneurs than US law. Europe takes a unified approach to the issue of intermediary liability, setting the same standard for holding intermediaries liable, regardless of the nature of the underlying offence. There is logic to this approach, even if it is unlike the American approach, which, as noted, offers different rules for intermediary liability for copyright, trademark and other offences.[9] The European Union's Electronic Commerce Directive sets out what are essentially safe harbours from liability for specified intermediary activities, such as acting as a "mere conduit," "caching" or "hosting" (but not search services). Some countries go further, so as to include safe harbours for search engines and hyperlink providers (Verbiest et al. 2007). Yet, from the perspective of Internet intermediaries, these safe harbours remain inferior to the American ones, providing less protection from copyright, trademark, defamation and other claims. Some of the deficiencies of EU law vis-à-vis US law for Internet intermediaries are explained here.[10]

First, the European approach stops far short of the near-blanket exclusion from liability offered by the CDA for non–intellectual property related wrongs.[11] Second, the EU's Electronic Commerce Directive largely adopts the DMCA's notice-and-takedown approach, but leaves open the possibility of additional proactive responsibilities on the part of the online intermediary. Even while disavowing any duty to "monitor," the EU law expressly contemplates the imposition by member states of "duties of care" on intermediaries to detect and prevent certain activities (European Parliament 2000). Third, the European directive lacks a statutory notice-and-takedown regime, creating greater uncertainty among European providers as to whether they have somehow acquired sufficient knowledge to be held liable if they do not delete material on their own (Peguera 2009, 490).

The two directives proved inferior to their US counterparts from the perspective of ISPs for the opposite reasons — the first for lack of specificity, and the second for too much specificity. While the Electronic Commerce Directive followed the DMCA's Title II in granting ISPs certain immunities arising from web-hosting activities, it did not specify the exact circumstances that would guarantee freedom from liability. Nor did the directive offer immunity to search engines (Kuczerawy and Ausloos 2015). At the same time, the very specificity of the directive undermined

8 *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997).

9 The Europeans describe their approach as a "horizontal" one, encompassing secondary liability for all illicit behaviour (Peguera 2009, 482–84).

10 I do not mean to suggest that European law is invariably hostile to Internet intermediaries. For example, an Italian court recently rejected an attempt to hold Google liable for the automatically generated suggestions of additional search terms that happened to add offensive words after a person's name (Coraggio 2013).

11 See Pfanner (2010), who quotes a London lawyer as saying, "The issue of when a host was liable has been getting a bit vague, and some hosts in Europe have been getting a little bit nervous."

its usefulness to web enterprises. Rather than an open-ended doctrine of fair use, EU law allowed only specified exceptions to the exclusive rights of the copyright holder.[12] These proved less flexible in responding to technological developments than did US fair use, which allowed a court to consider each new case individually, based on multiple factors. As one British scholar notes, fair use "provide[d] the courts with some flexibility of response to change in the way copyright works are disseminated and used, whether arising from new technologies, social behavior or institutional structures" (MacQueen 2009, 209; see also Hargreaves 2011).

Even as late as 2008, European lawyers could only advise that "The scope of liability of Web 2.0 websites is an unsettled point of law" (Joslove and De Spiegeleer-Delort 2008). It was not until 2012 that the European Court of Justice made clear that Internet intermediaries would not be required to affirmatively filter their entire networks for copyright infringement. In cases brought by the Belgian collecting society SABAM against the Internet access provider Scarlet and the online social network Netlog, the court held that enjoining these companies to filter uploads by all users on behalf of copyright owners would violate the privacy and speech rights of users, and would be unduly costly and burdensome to the Internet enterprise.[13] While the judgments in *SABAM v. Netlog* and *Scarlet v. SABAM* clearly support Web 2.0 enterprises, they arrived nearly a decade after the rise of such companies in the United States.

INTERMEDIARY LIABILITY LAW IN JAPAN

In Japan, running a bulletin board service in 1997 might render you liable for defamation occurring on that service. That year, a Tokyo trial court held Nifty Service, an ISP, liable for failing to delete defamatory messages (Tanaka 2001, 67). A heated exchange on a forum titled "Contemporary Ideas" had resulted in defamatory posts, which the forum's manager left up, "apparently believing that continuing the discussion and trying to engage the parties in a more issue-oriented dialogue would address the problem" (Mehra 2007, 801). It was not until 2001 that the Tokyo High Court would reverse the decision.

That same year, Japan's Diet passed the Law Concerning the Limits of Liability for Damages of Specified Telecommunications Service Providers, under which a telecommunications service provider would not be liable for the actions of its users unless it knew, or where there was "reasonable ground to find that said relevant service provider could know[,] the violation of the rights of others was caused by the information distribution via said specified telecommunications."[14] Like the European approach, the law applies to all intermediary activity, whether involving copyright, trademark or tort claims. By imposing not only an actual knowledge-and-takedown approach but also a more vague "reasonable ground" that the provider "could know," the 2001 limitation law was a pale shadow of the CDA Section 230 from the perspective of Internet enterprise.

In Japan, developing a peer-to-peer file-sharing service in the last decade might get you arrested. In 2002, Isamu Kaneko, a researcher at the University of Tokyo's School of Information and Science Technology, began distributing a peer-to-peer file-sharing program he wrote called "Winny." In May 2004, he was arrested for copyright infringement because he continued to distribute his program despite being aware that some had used it to infringe copyrights (*Daily Yomiuri* 2004). After his arrest, Kaneko, described as an "idol" among programmers, and who had taught a series of lectures to nurture "superprogrammers," resigned from his university position. In December 2006, the Kyoto District Court found him guilty, decrying his "selfish and irresponsible attitude," and concluding that he knew that Winny "was being used to violate the law and allowed users to do so" (*Daily Yomiuri* 2006). Yet, the judge conceded that "Kaneko did not specifically intend to cause copyright violations on the Internet" (ibid.). He was fined 1.5 million yen for the infringement. The Japanese Supreme Court would ultimately clear him of all charges, but not until December 2011 (*Japan Times* 2011).

Japan's 2001 law limiting liability for ISPs in certain circumstances was far less friendly to such companies than the DMCA. Rather than the relatively clear safe harbours of the DMCA, Japan's law removed any protections if the provider knew *or should have known* of infringement occurring through its service, a far more uncertain standard, especially given the likelihood that some users will infringe on any Web 2.0 service.

12 "This more restrictive approach limits the room to manoeuvre for the courts. The District Court of Hamburg, for instance, refused to bring thumbnails of pictures displayed by Google's image search service under the umbrella of the right of quotation" (Senftleben 2010, 536).

13 Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, paras. 46–48 (Feb. 16, 2012), available at http://curia.europa.eu/juris/celex.jsf?celex=62010CJ0360&lang1=en&type=TXT&ancre=; Case C-70/10, *Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Éditeurs SCRL (SABAM)*, 2011 E.C.R. I-11959, paras. 48, 52 (Nov. 24, 2011), available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62010CJ0070&from=EN.

14 Tokutei denkitsuushin ekimu teikyousha no songaibaishou sekinin no seigen oyobi hasshinsha jouhou no kaiji ni kansu ru houritsu [Law Concerning the Limits of Liability for Damages of Specified Telecommunications Service Providers and the Right to Request Disclosure of Identification Information of the Senders], Law No. 137 of 2001, art. 3, translated at www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/Compensation-Law.pdf (Japan).

INTERMEDIARY LIABILITY AND THE IMPACT ON INNOVATION

Imagine the boardroom in a Silicon Valley venture capital firm, circa 2005. A start-up less than a year old has already attracted millions of users. Now that start-up, which is bleeding money, needs an infusion of cash to survive and grow. The start-up allows users to share text, photos and videos, and includes the ability to readily share text, pictures and videos posted by friends. If that start-up can be accused of abetting copyright infringement on a massive scale, or must police its content like a traditional publishing house, lest it face damages claims or an injunction, the firm's US$100 million investment might go to plaintiffs' lawyers in damages and fees.[15] A court injunction might stop the site from continuing without extensive human monitoring, which could not be justified by potential revenue. Because of the insulation brought by US law reforms in the 1990s, American start-ups did not fear such a mortal legal blow. The legal privileges granted to Internet enterprises in the United States helped start-ups bridge the so-called "valley of death," the stage between creative idea and successful commercialization, in which most start-up enterprises founder.

While many European and Asian nations leave intermediaries open to liability for the actions of their users in certain cases, the United States generally limits liability. Liability limitations in the United States allowed the firms of Silicon Valley to worry about improving and expanding features and attracting and retaining customers, rather than policing their services for fear of lawsuits. The success of US Internet companies has depended not only on well-educated entrepreneurs and the availability of venture capital, but also on laws that reduced the legal risks in building platforms for the use of millions.

The example of public Wi-Fi in Germany helps dramatize the relationship of intermediary liability and the decision to offer a service. It has long been difficult to find public Wi-Fi in Germany. This is not for lack of technology in the country, but rather because of the law making Wi-Fi intermediaries liable for the actions of their users: "Private hotspot providers in Germany are liable for the misconduct of users. If, for example, a user were to download music or a movie on a particular hotspot, the provider ran the risk of being sued for piracy" (Brady 2016). Demands for compensation for copyright piracy made against ISPs abounded — "regardless of whether the provider was aware of the activity" (Moody 2016). When a German non-profit organization opened up its Wi-Fi to the public and someone used it illegally, "members of our office had an awkward interview at the police," it reported (Foundation for a Free Information Infrastructure 2015). The European Court of Justice is currently considering the issue of the liability of a free public Wi-Fi operator for copyright infringement (Masnick 2016). In May 2016, the German government lifted the spectre of liability, but it may be a while before individuals and businesses feel confident that they will not be liable in offering free Wi-Fi.

SURVEILLANCE AND LAW ENFORCEMENT

Information intermediaries have found themselves at the centre of another controversy — that of governmental surveillance. Because intermediaries gather a tremendous amount of data about users in their ordinary course of conduct, governments may seek that data for surveillance and other law-enforcement purposes. If the information is stored in one country but demanded by another — the laws of the two countries may come into conflict. The privacy laws of one country may interfere with the law-enforcement provisions of another. As David Kris (2015) describes:

> For example, a U.S. provider that stores data in the United States, from the email account of a British citizen located in England, might be simultaneously required (by DRIPA [the UK Data Retention and Investigatory Powers Act 2014]) and forbidden (by ECPA/SCA [the US Electronic Communications Privacy Act/Stored Communications Act]) to produce the email. Correspondingly, a U.S. provider that stores email abroad might be simultaneously required (by the SCA) and forbidden (by a foreign data protection law) to produce the email.

Laws vary widely on the steps necessary before a government authority can require an intermediary to turn over information about its users. While the revelations of Edward Snowden cast American practices in a negative light, laws around the world can also be problematic. A study for the Council of Europe reports that even in some of its member states, "Administrative authorities, police authorities or public prosecutors are given specific powers to order internet access providers to block access without advance judicial authority. It is common to see such orders requiring action on the part of the internet access provider within 24 hours, and without any notice being given to the content provider or host themselves" (Swiss Institute of Comparative Law 2015, 3).

Eager to access the information that online intermediaries might have on those distributing information in their countries, authoritarian governments, in particular, have increasingly sought to require online intermediaries to store data within their countries, facilitating access by

15 This hypothetical scenario finds real-world inspiration in the origins of Pinterest (Lynley 2012; Tsukayama 2012).

their security services. In 2016, Iran's Supreme Council for Cyberspace, for example, ordered messaging apps to store data within the country (Reuters 2016c). This follows a broad data localization mandate issued by the Russian government in 2015. Such data localization requirements facilitate a government's access to data by preventing the intermediary from shielding efforts to turn over data held abroad based on jurisdiction.

MANILA PRINCIPLES: BEST PRACTICES FOR REGULATING INTERNET INTERMEDIARIES

In 2015, a group of civil society organizations, including the Electronic Frontier Foundation, the Centre for Internet Society India and Article 19, proposed the "Manila Principles on Intermediary Liability." The Manila Principles are a set of best practices guidelines for limiting intermediary liability for content to promote freedom of expression and innovation. The six Manila Principles are:

> Intermediaries should be shielded by law from liability for third-party content.
>
> Content must not be required to be restricted without an order by a judicial authority.
>
> Requests for restrictions of content must be clear, be unambiguous, and follow due process.
>
> Laws and content-restriction orders and practices must comply with the tests of necessity and proportionality.
>
> Laws and content restriction policies and practices must respect due process.
>
> Transparency and accountability must be built into laws and content restriction policies and practices.[16]

The Manila Principles focus on due process, including the requirement of judicial orders for content takedown, as well as transparency and accountability. The principles have attracted early support in the human rights community. David Kaye (2015, 19), UN special rapporteur on free expression, observes, "The recently adopted Manila Principles on Intermediary Liability, drafted by a coalition of civil society organizations, provide a sound set of guidelines for States and international and regional mechanisms to protect expression online."

16 See www.eff.org/files/2015/10/31/manila_principles_1.0.pdf.

RIGHTS AND RESPONSIBILITIES: PRIVACY, HARMFUL SPEECH AND PRIVATE CONTROL

At the same time that Internet intermediaries help us as individuals connect, learn and converse, they also gain a tremendous amount of information about us and can, if they wish, exercise control over what we share and read. Thus, while freeing Internet intermediaries from liability for what their users do, we might still be concerned about what the intermediaries themselves do.

Many of the concerns raised with Internet intermediaries have revolved around privacy because of the tremendous data sets that they acquire. In the United States, the Federal Trade Commission has entered into settlements with Facebook, Google, Snapchat and Twitter whereby those companies pay for independent privacy audits conducted on a biannual basis for 20 years. These audits seek to ensure that these companies comport themselves according to the privacy promises they make in their terms of use.

Recently, some have worried that Internet intermediaries might manipulate the information on their services. These companies must also take care not to manipulate unfairly the information we receive through their services. They should also attend to the ways that automated algorithms can reinforce societal hierarchies (Chander, forthcoming 2017).

Facebook, Google, Twitter and others have increasingly been called upon to block the social media accounts of entities allegedly associated with international terrorism. Israel's security head has called Facebook a "monster" because it sets "a very high bar for removing inciteful content and posts" (Reuters 2016b). The Council of Europe, however, has cautioned member states to "ensure that their legal frameworks and procedures in this area are clear, transparent and incorporate adequate safeguards for freedom of expression and access to information in compliance with Article 10 of the European Convention on Human Rights" (Council of Europe 2016). Microsoft has issued a policy announcing its approach to online terrorist content. This is hardly a usual policy arena for a multinational company, but Microsoft's opening observation makes clear why this is necessary: "The Internet has become the primary medium for sharing ideas and communicating with one another and the events of the past few months are a strong reminder that the Internet can be used for the worst reasons imaginable" (Microsoft Corporation 2016). It amended its community guidelines to explicitly bar terrorist content, and stated that it would remove such content when it learned of it through a reporting system it provided online: "When terrorist content on our hosted consumer services is brought to our attention via our online reporting tool, we will remove it." To avoid becoming the arbiter of who is a terrorist ("There is no universally accepted definition of terrorist content,"

the company noted), Microsoft indicated that it would rely upon the list of organizations included on the Consolidated United Nations Security Council Sanctions List. Microsoft's policy seems a promising start, and its workability and consequences should be reviewed over time.

CONCLUSION

The Organisation for Economic Co-operation and Development (2010) concludes that Internet intermediaries increase user empowerment and choice, and improve purchasing power. Every second, some 2,534,097 emails are sent, 133,975 YouTube videos viewed, 56,896 Google searches conducted, 39,019 gigabytes of traffic posted through the Internet, 2,321 Skype calls made and 7,387 Tweets sent, according to estimates by the Internet Live Stats website.[17] The law regulating these and other online intermediaries helps determine whether such services are possible.

WORKS CITED

Article 19. 2013. *Internet Intermediaries: Dilemma of Liability*. Article 19. www.article19.org/data/files/Intermediaries_ENGLISH.pdf.

Box, Sarah and Jeremy West. 2016. "Economic and Social Benefits for Internet Openness." OECD Background Paper. doi:10.1787/5jlwqf2r97g5-en.

Brady, Kate. 2016. "Germany to Abolish Provider Liability Law, Open Path to More Free Wifi." DW, May 11. www.dw.com/en/germany-to-abolish-provider-liability-law-open-path-to-more-free-wifi/a-19249024.

Brouwer, Bree. 2015. "YouTube Now Gets Over 400 Hours of Content Uploaded Every Minute." TubeFilter, July 26. www.tubefilter.com/2015/07/26/youtube-400-hours-content-every-minute.

Chander, Anupam. 2014a. "How Law Made Silicon Valley." *Emory Law Journal* 63 (3): 639–94.

———. 2014b. "Law and the Geography of Cyberspace." *World Intellectual Property Organization* Journal 6 (1): 99–106.

———. Forthcoming 2017. "The Racist Algorithm?" *Michigan Law Review* 115.

Chander, Anupam and Uyen P. Le. 2014. "Free Speech." *Iowa Law Review* 100 (2): 501–49.

Coraggio, Giulio. 2013. "Google NOT Liable for Suggest Search Results." *GamingTechLaw* (blog), January 4. www.gamingtechlaw.com/2013/04/google-not-liable-for-suggest-search.html.

Council of Europe. 2016. "Rules for Blocking and Removal of Illegal Content Must be Transparent and Proportionate." Council of Europe, June 1. www.coe.int/en/web/human-rights-rule-of-law/-/rules-for-blocking-and-removal-of-illegal-content-must-be-transparent-and-proportionate.

Daily Yomiuri. 2004. "File-Sharing Author Arrested." *Daily Yomiuri*, May 11, 2.

———. 2006. "Winny Inventor Convicted." *Daily Yomiuri*, December 14, 1.

Dunai, Marton. 2016. "Hungary Passes Law that Could Block Uber Sites." Reuters, June 13. www.reuters.com/article/us-uber-hungary-ban-idUSKCN0YZ1KD.

European Parliament. 2000. *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.*

Foundation for a Free Information Infrastructure. 2015. "The German Störerhaftung of Wifi." *FFII* (blog), March 27. https://blog.FFII.org/the-german-storerhaftung-of-wifi/.

Hargreaves, Ian. 2011. *Digital Opportunity: Review of Intellectual Property and Growth.* UK Department for Business, Innovation & Skills. May 18. www.gov.uk/government/uploads/system/uploads/attachment_data/file/32563/ipreview-finalreport.pdf.

Japan Times. 2011. "Absurd Arrest Rectified." *Japan Times*, December 26 (editorial). www.japantimes.co.jp/opinion/2011/12/26/editorials/absurd-arrest-rectified/#.UlVbMGSSxJs.

Joslove, Bradley L. and Vanessa De Spiegeleer-Delort. 2008. "Web 2.0: Aggregator Website Held Liable as Publisher." International Law Office, June 26. www.internationallawoffice.com/newsletters/detail.aspx?g=4b014ec1-b334-4204-9fbd-00e05bf6db95#11.

Katyal, Neal Kumar. 2001. "Criminal Law in Cyberspace." *University of Pennsylvania Law Review* 149 (4): 1003–114.

Kaye, David. 2015. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.* Human Rights Council, May 22. A/HRC/29/32.

Kris, David. 2015. "Preliminary Thoughts on Cross-Border Data Requests." *LawFare* (blog), September 28. www.lawfareblog.com/preliminary-thoughts-cross-border-data-requests.

Kuczerawy, Aleksandra and Jef Ausloos. 2015. *European Union and Google Spain.* https://publixphere.net/i/noc/page/OI_Case_Study_European_Union_and_Google_Spain.

17 As of October 25, 2016. See www.internetlivestats.com/one-second/.

LaRue, Frank. 2011. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.* Human Rights Council, May 16. A/HRC/17/27.

Lemley, Mark A. 2007. "Rationalizing Internet Safe Harbors." *Journal on Telecommunications and High Technology Law* 6: 101, 102–5.

Lynley, Matt. 2012. "Pinterest: We're Not Going to Be Sued into Oblivion, and Here's Why." Business Insider, March 9. www.businessinsider.com/pinterest-were-not-going-to-be-sued-into-oblivion-and-heres-why-2012-3.

MacKinnon, Rebecca, Elonnai Hickok, Allon Bar and Hae-in Lim. 2014. *Fostering Freedom Online: The Role of Internet Intermediaries*. United Nations Educational, Scientific and Cultural Organization Report. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.

MacQueen, Hector L. 2009. "'Appropriate for the Digital Age'? Copyright and the Internet: 2. Exceptions and Licensing." In *Law and the Internet*, edited by Lilian Edwards and Charlotte Waelde, 183–225. Oxford, UK: Hart Publishing.

Masnick, Mike. 2016. "EU Court Of Justice Advocate General Says Open WiFi Operators Shouldn't Be Liable For Infringement." *TechDirt* (blog), March 17. www.techdirt.com/blog/wireless/articles/20160316/13090133923/eu-court-justice-advocate-general-says-open-wifi-operators-shouldnt-be-liable-infringement.shtml.

Mehra, Salil K. 2007. "Post a Message and Go to Jail: Criminalizing Internet Libel in Japan and the United States." *University of Colorado Law Review* 78 (3): 767–816.

Microsoft Corporation. 2016. "Microsoft's Approach to Terrorist Content Online." *Microsoft Corporate Blogs* (blog), May 20. http://blogs.microsoft.com/on-the-issues/2016/05/20/microsofts-approach-terrorist-content-online/#sm.0000v683y7u6hf1vzq116lgebcm77.

Moody, Glyn. 2016. "Germany Plans to Remove Owner Liability for Piracy on Open Wi-Fi Hotspots — Report." Ars Technica, May 13. http://arstechnica.co.uk/tech-policy/2016/05/german-open-wi-fi-storehaftung-law-repealed.

Organisation for Economic Co-operation and Development. 2010. *The Economic and Social Role for Internet Intermediaries.* April. www.oecd.org/internet/ieconomy/44949023.pdf.

Peguera, Miquel. 2009. "The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems." *Columbia Journal of Law & the Arts* 32 (4): 481–512.

Pfanner, Eric. 2010. "YouTube Can't Be Liable on Copyright, Spain Rules." *New York Times*, September 24, B7.

Reuters. 2016a. "Brazil Court Blocks Facebook Funds Over WhatsApp Dispute: Report." Reuters, June 30. www.reuters.com/article/us-brazil-facebook-whatsapp-idUSKCN0ZH3EX.

———. 2016b. "Israeli Minister Says Facebook a 'Monster', Hindering Security." Reuters, July 2. www.reuters.com/article/us-israel-facebook-idUSKCN0ZI0XB.

———. 2016c. "Iran Orders Social Media Sites to Store Data Inside the Country." Reuters, May 29. www.reuters.com/article/internet-iran-idUSL8N18Q0IN.

Risen, Tom. 2016. "Turkey Censors News, Social Media After Terrorist Attack." US News, June 29. www.usnews.com/news/articles/2016-06-29/turkey-censors-news-twitter-facebook-after-terror-attack.

Senftleben, Martin. 2010. "Bridging the Differences Between Copyright's Legal Traditions — The Emerging EC Fair Use Doctrine." *Journal Of the Copyright Society of the USA.* 57 (3): 521–52.

Swiss Institute of Comparative Law. 2015. "Comparative Study on Blocking, Filtering and Take-Down of Illegal Content." ISDC, December 20. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168068511c.

Tanaka, Hisanari Harry. 2001. "Post-Napster: Peer-to-Peer File Sharing Systems: Current and Future Issues on Secondary Liability Under Copyright Laws in the United States and Japan." *Loyola of Los Angeles Entertainment Law Review* 22 (1): 37–84.

Tsukayama, Hayley. 2012. "Pinterest Addresses Copyright Concerns." *Washington Post*, March 15. http://articles.washingtonpost.com/2012-03-15/business/35447213_1_ben-silbermann-pinterest-content.

United Nations. 1948. *Universal Declaration of Human Rights.* Geneva, Switzerland: United Nations. www.un.org/en/universal-declaration-human-rights/.

UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression, and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information. 2011. "Joint Declaration on Freedom of Expression and the Internet." www.osce.org/fom/78309?download=true.

Verbiest, Thibault, Gerald Spindler, Giovanni Maria Riccio and Aurelie Van der Perre. 2007. "Study on the Liability of Internet Intermediaries." November 12. http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf.

CIGI PUBLICATIONS
ADVANCING POLICY IDEAS AND DEBATE

Global Commission on Internet Governance

The Global Commission on Internet Governance (GCIG) was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem. Launched by two independent global think tanks, the Centre for International Governance Innovation and Chatham House, the GCIG will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

Global Commission on Internet Governance Paper Series

The Regime Complex for Managing Global Cyber Activities
GCIG Paper Series No. 1
Joseph S. Nye, Jr.

Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate
GCIG Paper Series No. 2
Tim Maurer and Robert Morgus

Legal Mechanisms for Governing the Transition of Key Domain Name Functions to the Global Multi-stakeholder Community
GCIG Paper Series No. 3
Aaron Shull, Paul Twomey and Christopher S. Yoo

Legal Interoperability as a Tool for Combatting Fragmentation
GCIG Paper Series No. 4
Rolf H. Weber

Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem
GCIG Paper Series No. 5
Stefaan G. Verhulst, Beth S. Noveck, Jillian Raines and Antony Declercq

The Impact of the Dark Web on Internet Governance and Cyber Security
GCIG Paper Series No. 6
Tobby Simon and Michael Chertoff

On the Nature of the Internet
GCIG Paper Series No. 7
Leslie Daigle

Understanding Digital Intelligence and the Norms That Might Govern It
GCIG Paper Series No. 8
David Omand

ICANN: Bridging the Trust Gap
GCIG Paper Series No. 9
Emily Taylor

A Primer on Globally Harmonizing Internet Jurisdiction and Regulations
GCIG Paper Series No. 10
Michael Chertoff and Paul Rosenzweig

Connected Choices: How the Internet is Challenging Sovereign Decisions
GCIG Paper Series No. 11
Melissa E. Hathaway

Solving the International Internet Policy Coordination Problem
GCIG Paper Series No. 12
Nick Ashton-Hart

Net Neutrality: Reflections on the Current Debate
GCIG Paper Series No. 13
Pablo Bello and Juan Jung

Addressing the Impact of Data Location Regulation in Financial Services
GCIG Paper Series No. 14
James M. Kaplan and Kayvaun Rowshankish

Cyber Security and Cyber Resilience in East Africa
GCIG Paper Series No. 15
Iginio Gagliardone and Nanjira Sambuli

Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime
GCIG Paper Series No. 16
Eric Jardine

CIGI PUBLICATIONS
ADVANCING POLICY IDEAS AND DEBATE

The Emergence of Contention in Global Internet Governance
GCIG Paper Series No. 17
Samantha Bradshaw, Laura DeNardis, Fen Osler Hampson, Eric Jardine and Mark Raymond

Landmark EU and US Net Neutrality Decisions: How Might Pending Decisions Impact Internet Fragmentation?
GCIG Paper Series No. 18
Ben Scott, Stefan Heumann and Jan-Peter Kleinhans

The Strengths and Weaknesses of the Brazilian Internet Bill of Rights: Examining a Human Rights Framework for the Internet
GCIG Paper Series No. 19
Carolina Rossini, Francisco Brito Cruz and Danilo Doneda

The Tor Dark Net
GCIG Paper Series No. 20
Gareth Owen and Nick Savage

The Dark Web Dilemma: Tor, Anonymity and Online Policing
GCIG Paper Series No. 21
Eric Jardine

One in Three: Internet Governance and Children's Rights
GCIG Paper Series No. 22
Sonia Livingstone, John Carr and Jasmina Byrne

Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity
GCIG Paper Series No. 23
Samantha Bradshaw

The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality
GCIG Paper Series No. 24
Emily Taylor

The Digital Trade Imbalance and Its Implications for Internet Governance
GCIG Paper Series No. 25
Susan Ariel Aaronson

A Pragmatic Approach to the Right to Be Forgotten
GCIG Paper Series No. 26
Kieron O'Hara, Nigel Shadbolt and Wendy Hall

Education 3.0 and Internet Governance: A New Global Alliance for Children and Young People's Sustainable Digital Development
GCIG Paper Series No. 27
Divina Frau-Meigs and Lee Hibbard

Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation
GCIG Paper Series No. 28
Bertrand de La Chapelle and Paul Fehlinger

Patents and Internet Standards
GCIG Paper Series No. 29
Jorge L. Contreras

Tracing the Economic Impact of Regulations on the Free Flow of Data Localization
GCIG Paper Series No. 30
Matthias Bauer, Martina F. Ferracane and Erik van der Marel

Looking Back on the First Round of New gTLD Applications: Implications for the Future of Domain Name Regulation
GCIG Paper Series No. 31
Jacqueline D. Lipton

Governance of International Trade and the Internet: Existing and Evolving Regulatory Systems
GCIG Paper Series No. 32
Harsha Vardhana Singh, Ahmed Abdel-Latif and L. Lee Tuthill

Market-driven Challenges to Open Internet Standards
GCIG Paper Series No. 33
Patrik Fältström

How to Connect the Other Half: Evidence and Policy Insights from Household Surveys in Latin America
GCIG Paper Series No. 34
Hernán Galperin

A Framework for Understanding Internet Openness
GCIG Paper Series No. 35
Jeremy West

Internet Openness and Fragmentation: Toward Measuring the Economic Effects
GCIG Paper Series No. 36
Sarah Box

Why Are Two Networks Better than One? Toward a Theory of Optimal Fragmentation
GCIG Paper Series No. 37
Christopher S. Yoo

One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation
GCIG Paper Series No. 38
Laura DeNardis

Ethics in the Internet Environment
GCIG Paper Series No. 39
Rolf H. Weber

Standards, Patents and National Competitiveness
GCIG Paper Series No. 40
Michael Murphree and Dan Breznitz

Multi-stakeholderism: Anatomy of an Inchoate Global Institution
GCIG Paper Series No. 41
Mark Raymond and Laura DeNardis

Available for free download at www.cigionline.org/publications

CIGI
Centre for International Governance Innovation
www.cigionline.org

ABOUT CIGI

We are the Centre for International Governance Innovation: an independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis.

Our research programs focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners and support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

Au Centre pour l'innovation dans la gouvernance internationale (CIGI), nous formons un groupe de réflexion indépendant et non partisan qui formule des points de vue objectifs dont la portée est notamment mondiale. Nos recherches, nos avis et l'opinion publique ont des effets réels sur le monde d'aujourd'hui en apportant autant de la clarté qu'une réflexion novatrice dans l'élaboration des politiques à l'échelle internationale. En raison des travaux accomplis en collaboration et en partenariat avec des pairs et des spécialistes interdisciplinaires des plus compétents, nous sommes devenus une référence grâce à l'influence de nos recherches et à la fiabilité de nos analyses.

Nos programmes de recherche ont trait à la gouvernance dans les domaines suivants : l'économie mondiale, la sécurité et les politiques mondiales, et le droit international, et nous les exécutons avec la collaboration de nombreux partenaires stratégiques et le soutien des gouvernements du Canada et de l'Ontario ainsi que du fondateur du CIGI, Jim Balsillie.

For more information, please visit www.cigionline.org.

ABOUT CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is based in London. Chatham House's mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all. The institute: engages governments, the private sector, civil society and its members in open debates and confidential discussions about significant developments in international affairs; produces independent and rigorous analysis of critical global, regional and country-specific challenges and opportunities; and offers new ideas to decision-makers and -shapers on how these could best be tackled from the near- to the long-term. For more information, please visit: www.chathamhouse.org.

CIGI MASTHEAD

Executive

President	Rohinton P. Medhora
Director of Finance	Shelley Boettger
Director of the International Law Research Program	Oonagh Fitzgerald
Director of the Global Security & Politics Program	Fen Osler Hampson
Director of Human Resources	Susan Hirst
Director of the Global Economy Program	Domenico Lombardi
Chief of Staff and General Counsel	Aaron Shull
Director of Communications and Digital Media	Spencer Tripp

Publications

Publisher	Carol Bonnett
Senior Publications Editor	Jennifer Goyder
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Publications Editor	Sharon McCartney
Publications Editor	Lynn Schellenberg
Graphic Designer	Sara Moore
Graphic Designer	Melodie Wakefield

For publications enquiries, please contact publications@cigionline.org.

Communications

For media enquiries, please contact communications@cigionline.org.

CIGI
67 Erb Street West
Waterloo, Ontario N2L 6C2
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs
10 St James's Square
London, England SW1Y 4LE, United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org