Centre for International
Governance Innovation

Conference Report — Global Platform Governance Network Transparency Working Group

Transparency Recommendations for Regulatory Regimes of Digital Platforms

Mark MacCarthy

Centre for International
Governance Innovation

Conference Report — Global Platform Governance Network Transparency Working Group

Transparency Recommendations for Regulatory Regimes of Digital Platforms

Mark MacCarthy

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director of Digital Economy Robert Fay
Policy Lead, Platform Governance Chris Beall
Publications Editor Susan Bubak
Senior Publications Editor Jennifer Goyder
Graphic Designer Brooklynn Schwartz

The Balsillie Family Foundation and Reset provided financial support for this project.

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

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

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Global Platform Governance Network

CIGI and Reset (https://luminategroup.com/reset) partnered to create the Global Platform Governance Network (GPGN), which launched in late August 2020. The GPGN is a global community of civil servants, legislative staff and regulators committed to a collaborative and harmonized approach to address pressing challenges related to digital platform governance. GPGN members work across a broad range of issues (from regulating the digital economy to countering terrorism and disinformation) and come from more than 25 countries worldwide, including both Global North and Global South and multilateral organizations (for example, the Council of Europe, the Organisation for Economic Co-operation and Development and the United Nations Educational, Scientific and Cultural Organization). Monthly, closed-door GPGN meetings enable participants to discuss pressing platform governance challenges, gain a deeper understanding of policy-level solutions and form relationships with international peers for future collaborations.

In early 2021, the GPGN established three working groups, supported by international experts functioning as rapporteurs, to enable members to discuss and co-develop practical solutions that could then be implemented in members' home jurisdictions. These groups focused on harmonizing digital platform **transparency** and **regulation** work under way worldwide, aligning current government research efforts to avoid duplication and identify critical gaps, and identifying what constitutes "success" for platform governance and the **measurement** tools that could be used to track progress toward desired outcomes.

About the GPGN Transparency Working Group

In January 2021, the GPGN launched its Transparency Working Group at its regular monthly meeting, guest led by Delphine Halgand-Mishra, founding executive director of The Signals Network and CIGI senior fellow. The session featured Mark MacCarthy, adjunct professor and senior fellow at Georgetown University, and Raegan MacDonald, head of public policy, Mozilla. Key takeaways from the presentations and group discussions included: government interventions need to be tailor-made, evidence-based and practical; systemic transparency is a prerequisite to advancing digital platform accountability; and governments need to be precise about which transparency requirements they impose — and be focused and specific about what information is required and why. Participants concluded that there is a need for a well-funded, independent regulatory structure that provides insight, transparency, risk assessment and oversight. Regulators should understand the issues they are dealing with, communicate with and be able to probe digital platforms and other stakeholders to avoid information overload, and ensure that the regulations and obligations are effective and enforceable and serve a purpose.

Following this session, the network launched the working group, which met three times between March and July 2021, with support from Mark MacCarthy, Delphine Halgand-Mishra and Heidi Tworek. The working group included civil servants, regulators and regulatory staff from Europe, North America, Africa and the Asia-Pacific, as well as from multilateral agencies, with several members recommending colleagues from within their governments leading work on developing or implementing new regulations. Members shared their experiences and insights, learned from their international colleagues and identified the granular issues that governments and regulators need to address as they move forward to regulate digital platforms and enforce digital platform transparency measures.

This report sets out clear, practical advice for legislators, governments and regulators working to address digital platform governance challenges now and into the future.

About the Rapporteur

Mark MacCarthy is an adjunct faculty member in the Communication, Culture & Technology Program in the Graduate School at Georgetown University, where he teaches courses in technology policy. He also teaches courses on privacy and artificial intelligence (AI) ethics in the Philosophy Department. He is a senior fellow at the Institute for Technology Law and Policy at Georgetown Law and a senior policy fellow at the Center for Business and Public Policy at Georgetown's McDonough School of Business. He is a senior fellow at the Future of Privacy Forum, where he works on AI and data privacy projects, and a nonresident senior fellow in Governance Studies at the Center for Technology Innovation at Brookings. He holds a Ph.D in philosophy from Indiana University and an M.A. in economics from the University of Notre Dame.

Acronyms and Abbreviations

BAI	Broadcasting Authority of Ireland
CFPB	Consumer Financial Protection Bureau
CRTC	Canadian Radio-television and Telecommunications Commission
DPAs	data protection authorities
FCC	Federal Communications Commission
FTC	Federal Trade Commission
G7	Group of Seven
G20	Group of Twenty
GPGN	Global Platform Governance Network
ICN	International Competition Network
NGOs	non-governmental organizations
OECD	Organisation for Economic Co-operation and Development
Ofcom	Office of Communications
PACT Act	Platform Accountability and Consumer Transparency Act
SEC	Securities and Exchange Commission

Introduction

In 2021, the Centre for International Governance Innovation (CIGI) organized a working group of its Global Platform Governance Network (GPGN) to focus on the issues of transparency and accountability of digital platforms, especially social media networks. CIGI held three online meetings to discuss the different aspects of these regulatory tools, which are mandated in many of the legislative proposals from different jurisdictions aiming to improve online safety. Mark MacCarthy, adjunct professor at Georgetown University, opened each meeting with a short presentation to focus the discussion. The objective was to share knowledge of the aims, methods, problems, strengths and weakness of new transparency and accountability regimes, and to work toward a common understanding of effective approaches. This report attempts to synthesize and summarize the discussions at these meetings.

On March 26, 2021, the Transparency Working Group met to discuss the questions of transparency of what, transparency to whom and transparency for which businesses. The group identified content moderation, advertising and the operation of the platform's service as areas for disclosure. It discussed the different audiences for these disclosures, including the public, users, auditors, researchers and regulators. A major insight was that the extent of the disclosures should be targeted to the nature of the audience, with researchers and regulators receiving more information than the general public and individual users.

On May 27, 2021, the working group meeting focused on the governance system needed to enforce transparency rules. The group consensus was for a sector-specific independent digital regulator to head the enforcement effort, with strong supervisory powers. Heidi Tworek, associate professor at the University of British Columbia and CIGI senior fellow, presented to the group on the need for civil society to be actively engaged in the governance mechanism, rather than leave enforcement solely to the interaction of regulators and platforms. The group thought the era of pure self-regulation was over, but that strong government enforcement could be accomplished through co-regulatory efforts such as industry codes of conduct, perhaps crafted with input from civil society groups, and ultimately approved and supervised by a regulator.

On July 29, 2021, the group discussed international cooperation and democratic governance, featuring presentations from Kelly Tallon and Ella Serry with Australia's eSafety Commissioner, Celene Craig with the Broadcasting Authority of Ireland (BAI) and Ben Whitman with the United Kingdom's Department of Digital, Culture, Media, and Sport. A major takeaway in connection with international cooperation was the urgency and difficulty of achieving international consensus on a standardized way of implementing transparency requirements for global companies. On democratic governance, the group focused on the balance needed to allow the transparency regulators to be both independent of improper partisan interference and accountable to the government, the legislature, the courts and the public.

What Are Transparency Measures?

Transparency measures are one element in a larger regulatory framework for digital companies, including social media platforms. They require these companies to disclose certain information concerning their content moderation programs to their users, the public, regulators, auditors or researchers. These requirements work together with the larger regulatory program to achieve important public policy objectives: to protect users from unfair treatment in connection with the administration of content moderation programs; to encourage companies to spend more resources on these programs; to learn what works to counteract the harmful material, hate speech, terrorist material, misinformation and disinformation on these platforms; to measure compliance with regulatory requirements; and to guide regulators in developing further effective regulatory measures.

Governments crafting transparency rules should consider several dimensions of these requirements, which can be grouped under the rubrics of transparency of what, transparency to whom and transparency for which companies. Governments should mandate disclosures, but might want to tier the disclosure of different types of information depending on the nature, size or market position of the companies involved, the potential risks to society, and the intended recipients of the information to be disclosed.

The following list of mandated disclosures and reports is drawn from online regulation measures pending or in place in Australia, Canada, the European Union, Germany, Ireland, the United Kingdom and the United States. A list of these measures and other resources can be found in Appendix 2 at the end of this report.

The first area that needs to be considered is "transparency of what?" In order to ensure the fair operation of these programs, governments might want to require the disclosure of:

→ content rules (the types of content and activity not permitted on the service);

→ enforcement procedures (criteria for demotion, delay or deletion of content and suspension or termination of service);

→ notification process (how to notify the service of illegal or violative content);

→ explanations (reasons for content moderation action);

→ complaint process (for redress when content is removed, or not removed after notice);

→ misuse policy (for unfounded notifications or complaints); and

→ misuse warnings (prior to suspension or termination of accounts).

These disclosures would provide for due process protections when a digital company takes an enforcement action or fails to take one. They would be needed to ensure the effective functioning of an associated accountability mechanism such as an internal or external process of redress and review. Such reviews might show whether and how companies are living up to their codes.

In addition, the public and regulators need regular reports and disclosures concerning the operation of the content moderation program and its associated algorithms, including:

→ number of government orders on illegal content and action taken;

→ number of notices by type of illegal content and action taken;

→ number of content moderation actions by type and basis of measure;

→ number of complaints of improper content moderation, including reversals;

→ number of out-of-court disputes;

→ number of suspensions;

→ number of unfounded notifications;

→ number of unfounded complaints;

→ purpose and accuracy of content moderation algorithms;

→ main parameters;

→ technical detail; and

→ source code.

The purposes of these disclosures are to put public pressure on companies to do an effective job of moderating the content on their system and to highlight areas for improvement. These disclosures work together with other elements of a regulatory program such as content removal requirements. They would take direction from the companies in determining what and how they report. To be useful, mandated disclosures should conform to a common standard across governments and jurisdictions, which creates an urgent need for standards development work. As discussed later and displayed in Table 1 in Appendix 1, the details of content moderation algorithms and source code should be available only to the regulator.

Finally, information about the operation of the digital service and any associated advertising practices needs to be disclosed, with appropriate protections for sensitive trade secrets and personal information. This might include:

→ average monthly users;

→ monitoring and compliance data;

→ recommendation algorithms (how content is ordered, prioritized and recommended);

→ sensitive data (trade secrets, systemic risk assessments and user personal data);

→ content of the message, including identification as an ad;

- sponsorship (who is the beneficiary of the ad);
- audience (both total and targeted audience size);
- main targeting criteria (meaningful information on basis for receiving the ad); and
- algorithms (technical detail or source code).

Access to this information allows other regulatory measures to function effectively, including a requirement for independent audits and research by qualified researchers into the effectiveness of content moderation techniques and the role played by recommendation and advertising algorithms in the spread of harmful online material. As with the details of content moderation algorithms and source code, the details of operational and advertising algorithms and source code should be available only to regulators.

The second topic is "transparency for whom?" Disclosures of different types of information should be tiered in order to accomplish public policy objectives while protecting sensitive information. The key groups are the general public, users, auditors, researchers and regulators.

The policy objective of disclosure to the general public is consumer protection and public accountability. Information should be published for all to see when it is needed for the public to understand the nature of the online service provided, the company rules governing its use and whether the service is operating as described. Examples of public disclosure in proposed legislation include requirements for digital companies to publish their terms and conditions, complaint procedures, redress processes and regular transparency reports outlining the prevalence of harmful content on their platforms and what countermeasures they are taking to address them. Some proposals also require digital companies to maintain public repositories of political ads.

The policy objective of disclosure to the individual user is consumer protection. Individual users should have access to certain information to guide their interactions with the service in real time and to make use of notification or redress possibilities in a timely fashion. Governments might also want to require the companies to provide information about online ads to the recipient. Some of this information might be sensitive, such as the explanation for removal of content, and so the decision to make that information public should rest with the users, not the service provider.

Finally, the public policy objective of requiring disclosures to outside auditors is enforcing compliance with regulatory requirements, and generating recommendations for improvements, if necessary. Independent auditors need access to confidential company information to verify the accuracy of company disclosures and compliance with regulatory requirements. Audit reports, redacted of confidential information, should be published to promote public accountability.

In a similar way, regulators and researchers vetted by the regulators need access to confidential company data and algorithms to assess systemic threats to public policy objectives, the effectiveness of mitigation measures and regulatory compliance. These threats might include distribution of illegal content; violations of rights to freedom of expression and information, consumer protection, privacy and non-discrimination; or adverse impacts on public health, public safety or political governance. This might include access to information about content-selection and recommendation algorithms, as well as confidential and personal information that should be protected from public disclosure.

Table 1 in Appendix 1 provides an example of how transparency requirements might be tiered to different recipients in order to balance the need for disclosure with the needs of confidentiality.

The final dimension of a transparency regime is its scope or coverage. Transparency rules should define the types of companies to which the rules apply by line of business, by size or reach of company, by market position, or by some combination of these factors. The scope should be sufficiently clear so that companies know when they are affected, and flexible enough so that the agency can update the regulatory boundaries to accommodate technological or business changes in the rapidly evolving digital landscape.

Some proposals include all companies that allow users to share or discover user-generated content or interact with each other online, and so would cover messaging services and search engines as well as social media platforms. Others exclude messaging services or search engines, or both. Others have different requirements for hosting companies, online platforms and electronic marketplaces.

In addition, transparency requirements could differ based on a company's number of users or employees or a combination of firm size and reach in order to avoid excessive impacts on small firms. Germany's Network Enforcement Act, or NetzDG law, for instance, excludes companies with fewer than two million registered German users.[1] The European Commission's proposed Digital Services Act applies certain transparency requirements only to companies with more than 50 employees and others only to online platforms reaching more than 10 percent of the EU population or 45 million persons.[2] It excludes small companies from certain transparency rules unless they reach a large audience. Other measures might combine number of unique monthly users with a measure of annual revenues to define the scope of the transparency requirements.

Another determinant of scope might be market position. Transparency rules might apply only to companies with a dominant position or with bottleneck power. This measure is used in many regulatory proposals designed to rein in the economic power of dominant digital firms. For instance, the Australian News Media and Digital Platforms Mandatory Bargaining Code requires digital platforms with bottleneck power to pay fair compensation to news outlets.[3] The United Kingdom's proposed Digital Markets Unit would create rules for firms with strategic market power. The European Commission's proposed Digital Markets Act calls for rules for online gatekeepers with durable and strong economic and intermediation positions.[4] Applying transparency rules based on market power might be appropriate if policy makers determine that transparency requirements are especially important to protect consumers with a lack of realistic alternatives for obtaining an essential service.

Governance

A key question for a new regime for digital companies is who makes and enforces the rules and codes of conduct, including the rules regarding transparency. The choices are:

→ self-regulation (each platform makes and enforces its own rules);

→ industry regulation (an industry organization develops and enforces common rules);

→ co-regulation (an industry organization develops and enforces common rules but is authorized and supervised by a government regulator); and

→ government regulation (an authorized government agency makes and enforces transparency rules).

The advantages of the lower levels of regulation are flexibility and agility in the face of changing industry and technological realities. Government rulemaking can be slow and cumbersome and might not be able to react in time to meet urgent social needs. The advantage of the higher level of regulation is that companies must take certain steps under the compulsion of law, which often removes competitive, financial and coordination barriers preventing companies from acting in the public interest.

Policy makers need not abandon lower levels of governance as they move to mandatory requirements. A government regulator might choose to allow companies to use self-regulation or industry regulation to set, update and enforce industry rules, including transparency rules, while still retaining overall authority to step in and revise the industry rules as needed, to enforce standards on what and how information is disclosed, and to make sure personal and proprietary information is kept confidential. This is a common feature of financial regulation, where an industry organization such as the Financial Industry Regulatory Authority in the United States sets and enforces rules for brokers and dealers of securities subject to the ongoing supervision of the Securities and Exchange Commission (SEC).

All the proposed governance regimes for digital companies have moved away from sole or primary reliance on self- or industry regulation

[1] See https://germanlawarchive.iuscomp.org/?p=1245.

[2] See https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.

[3] See https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6652_first-reps/toc_pdf/20177b01.pdf.

[4] See https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

and toward regulation by a government agency. Often these proposals empower the regulator to work with covered companies and other stakeholders, including academics, think tanks and civil liberties organizations, to set enforceable codes of conduct. The experience of the last few years with self-regulatory codes has persuaded policy makers that they are not enough on their own to protect users and the public from online harms. The consensus seems to be that a digital regulatory agency is needed.

What should be the nature and role of this digital regulatory agency? Policy makers have several choices. One is an economy-wide regulator with a specific policy mission. Data protection authorities (DPAs) in many countries play this role. Except in the United States, which generally has a sectoral approach to privacy, DPAs have jurisdiction over all firms in the economy, but only for purposes of enforcing privacy rules. DPAs regulate digital firms with respect to their data practices, but they use generally applicable rules rather than data protection rules specifically designed for firms in a particular line of business. Competition authorities and consumer protection agencies function in the same way. They also have broad scope over firms no matter what products or services they provide, but only for the purpose of promoting competition or protecting consumers.

An alternative would be an industry-specific regulator with authority only over companies engaged in certain digital lines of business, and not others. In many jurisdictions, sector-specific agencies regulate media firms, communications carriers, energy companies and financial service firms, among others. The agencies are authorized to do this because these firms provide services that are central to public life and are unavoidable for citizens seeking to participate fully in the economic, social, political and cultural life of their country. Often these agencies have subject matter jurisdiction that spans several policy areas, since their ultimate responsibility is to ensure that these essential businesses operate in the public interest. The US Federal Communications Commission (FCC), for instance, has authority to promote competition, protect privacy and enforce content rules for the telephone, broadcasting and cable companies under its jurisdiction. Financial regulators are also sector-specific in their focus, but with multiple missions. They aim to preserve safety and soundness of financial institutions, mitigate systemic risk and protect investors and financial consumers. In the United States, they also have responsibilities for information security and financial privacy.

The current proposals for governing digital companies all call for industry-specific regulation, with an agency authorized to protect users and the public from online harms created by companies in certain digital lines of business. Sometimes the proposals would house such a digital regulator in the agency responsible for traditional media regulation. The United Kingdom, for instance, has proposed expanding the authority of its current media regulator, the Office of Communications (Ofcom), to include responsibility for online safety. Ireland is looking to expand the role of the BAI to include a new online safety commissioner and would rename the expanded agency the Media Commission. Canada is seeking to expand the role of its media regulator, the Canadian Radio-television and Telecommunications Commission (CRTC), to supervise online broadcasting, but not to deal with online harms.

Some proposals would provide an economy-wide regulator with new authority over specifically digital issues. The proposed Platform Accountability and Consumer Transparency Act (PACT Act) in the United States,[5] for instance, would vest authority to supervise transparency requirements for social media companies with the Federal Trade Commission (FTC), which has economy-wide jurisdiction. In a related area of digital regulation, the United Kingdom has proposed the creation of a new Digital Markets Unit with regulatory authority to implement a pro-competition regime for digital markets, including social media companies, and it intends to house the new digital unit within the existing Competition and Markets Authority.

Other jurisdictions opt for a separate agency with sector-specific responsibilities for online safety. Several years ago, Australia created a brand-new agency, the eSafety Commissioner, to supervise online content, and legislation is moving forward to expand its powers.[6] Canada has proposed creating a new Digital Safety Commission, separate from its existing media regulator CRTC, to deal with online harms for a specific group of so-called online communication service providers.

[5] See www.congress.gov/bill/117th-congress/senate-bill/797/text.

[6] See www.esafety.gov.au/about-us/who-we-are/our-legislative-functions and www.esafety.gov.au/about-us/safety-by-design.

The European Commission takes a mixed approach. Its proposed Digital Services Act would regulate online harms throughout Europe and would require member countries to designate a digital services coordinator to apply the regulation. Its proposed Digital Markets Act would authorize the European Commission to monitor, implement and enforce special competition rules for digital gatekeepers. Its proposed AI regulation would require member states to designate national supervisory authorities to conduct market surveillance of AI products, but would not mandate the creation of new, specialized AI regulatory authorities.

The advantages of a new sector-specific digital regulator are greater agility and flexibility, the ability to develop industry expertise needed to tailor rules to the problems of the industry, and perhaps additional resources. Such a digital regulator would also be more likely to take a fresh approach unfettered by agency traditions to meet the evolving challenges of digital industries. In contrast, it would be easier and less costly to expand the mandate of a traditional agency. The established agency could also draw on existing agency resources and experiences in meeting its new regulatory challenges.

Another challenge would be dealing with the overlap among policy areas. Some measures that promote good content moderation sometimes also promote privacy protection and competition, but sometimes they are in tension with these other goals. The United Kingdom deals with these synergies and tensions by setting up a digital regulatory cooperation forum, linking the separate agencies responsible for privacy, digital competition and online safety in a non-statutory arrangement to coordinate the actions they take in pursuit of their separate missions. But if these synergies and tensions among content moderation, privacy and competition are commonplace, rather than rare or isolated corner cases, a coordinating mechanism that relies on consultations among independent regulators with no common decision maker might not be able to reach a balanced result. A single digital regulator with responsibilities for all three policy areas might do a better job of developing the policy tools that reinforce the separate missions and avoiding the measures that create or exacerbate conflicts.

Democratic Oversight

The institutional structure of the new digital regulator must build in democratic oversight that provides for both independence and accountability. A crucial task in the design of any regulatory institution is getting the balance right between the independence that allows for non-partisan regulatory determinations and the oversight that provides for public accountability. But it is especially critical for a digital agency where a significant risk of partisan abuse exists because the agency will be required to make decisions closely related to controversial social media content as part of implementing transparency rules.

The independence of a digital regulator depends in large part on its relationship to the current administration or government. Some regulatory agencies are departments or ministries that are fully integrated into the current administration. In the United States, agencies such as the Occupational Safety and Health Administration, the Environmental Protection Agency and the Consumer Financial Protection Bureau have this form. In contrast, independent regulatory agencies are not under the control of or supervised by any other body of the current government. The FCC, the FTC and the SEC are US examples. In other jurisdictions, data protection authorities and media regulators are independent from the incumbent government.

This autonomy from other governmental bodies has three dimensions: operational independence, financial independence and leadership independence. Operational independence means that the regulatory authority is not permitted to seek or take instructions from any other body of the current government in performing its tasks. Its decisions are not reviewable or subject to modification or repeal by the current government. Financial independence provides that the agency's budget is not subject to the control of another administrative agency in the government. Revenue to fund agency operations comes from a legislative appropriation, or industry fees. Under leadership independence, the agency's leaders cannot be removed by the existing government, except for cause, which includes inefficiency, neglect of duty or malfeasance in office or other failure to fulfill the conditions required for the performance of their duties. Leadership independence controls the risk that the current government would seek to directly influence agency actions by removing and replacing its directors.

In the United States, a recent Supreme Court decision involving the structure of the Consumer Financial Protection Bureau (CFPB) created a trade-off in the design of regulatory agencies. The members of a multi-member commission can be removed only for cause; in contrast, the director of a single-administrator agency serves at the will of the president. In the United States, only a bare majority of the members of a multi-member commission can be from the same political party and decisions are made by majority vote. As a result, commissions are less agile and efficient in reaching and adjusting their decisions, but more independent than single-administrative agencies. The ideal might be the efficiency of a single administrator and the independence of a multi-member commission, which was how the CFPB was originally organized. But in the United States, the Supreme Court has ruled out that possibility.

Under the United Kingdom's online safety bill, the responsibility for enforcing the new transparency measures is largely in the hands of the independent media regulator, Ofcom, even though the secretary of state has significant authority. Under the proposed online safety bill in Australia, the independent eSafety Commissioner would continue to be responsible for online safety measures and would receive substantially enhanced enforcement powers.[7] The proposed US PACT Act would authorize the independent FTC to enforce its new social media transparency mandates.

Another important democratic safeguard for a digital regulatory agency is accountability. The agency should not be set up so that it can become a law unto itself, able to act without any supervision or oversight at all. Several features of agencies with substantial independence could provide for this needed accountability. In the United States, the president nominates the members of independent commissions and designates one of them as the chair. The president can remove any of the commissioners for cause and can replace the chair with another sitting member of the commission at will. This provides a mechanism for the current administration to set the regulatory agenda of the commission by choosing a chair with compatible views, while still preventing direct influence over particular agency decisions. The commission structure with its requirement of a majority vote and bipartisan composition also tends to assure that regulatory measures will have a broad appeal, reflecting a rough consensus in the policy community.

Legislative bodies provide accountability through their substantial control over independent agencies. They provide the funding for the agencies, often approve its leadership and conduct public oversight hearings of agency activities. Legislatures can withdraw authority from agencies and restrict their ability to engage in certain regulatory activities. In some jurisdictions, they can override agency decisions in particular cases. They often require regular public reports from the agencies on the conduct of their regulatory mission and can insist that the agencies conduct their meetings and make their decisions in public.

Courts also have substantial authority over agency actions and decisions. They can review decisions to make sure fair procedures were followed, to prevent arbitrary or capricious actions, to ensure that agency actions are within its statutory authority, and to assess decisions for consistency with constitutional or human rights principles. These independent judicial reviews, separate from administrative review by another body of the current government, provide an important public check on agency discretion.

Democratic oversight of a regulatory regime for social media transparency is a thorny issue. It requires carefully crafting the duties and responsibilities of the agency responsible for transparency enforcement. Done right, it can provide for both independence from illegitimate partisan interference with the agency mission and accountability to the public, to legislative bodies and to the courts.

[7] See www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6680.

International Cooperation

The major online companies subject to transparency requirements operate in many jurisdictions at the same time and often provide platforms for cross-border transactions and exchanges. It would be desirable for digital regulators to have a similar international reach. This might help to prevent agencies from acting at cross purposes with each other, make compliance easier for the social media companies and produce information that is useful across jurisdictions. As a first step, national digital regulators should develop an institutional structure that allows them to share ideas and experiences related to their regulatory responsibilities and to develop a common understanding of the purposes, scope and implementation issues connected to transparency rules. Unlike substantive content rules, which inevitably will be national in character, transparency rules ultimately might be harmonized.

One model for such an institutional structure for regulatory cooperation is what the Organisation for Economic Co-operation and Development (OECD) calls transgovernmental networks. These networks provide loosely structured ties among specialized regulators developed through frequent interaction, informal but structured dialogues and regular meetings. Some examples include the International Organization of Securities Commissions, the Financial Action Task Force, the Basel Committee on Banking Supervision, the International Consumer Protection and Enforcement Network and the International Competition Network (ICN).

Some of these networks, such as the ICN, serve simply to exchange ideas and experiences so that regulators in different countries understand each other's approaches and priorities in their common domain of jurisdiction. Other networks, such as the Basel Committee, aim to set common standards that they can apply in their domestic regulatory activity.

Another possibility for digital regulatory cooperation would be through the Group of Seven (G7) and Group of Twenty (G20) groups. These groups regularly develop common principles in areas of mutual concern. The G7 has already taken some steps toward coordination of transparency requirements for digital companies. In April 2021, it issued a digital and technology ministerial declaration that contained an important agreement on internet safety principles, including a general principle on transparency and accountability. Building on this cooperation, the United Kingdom will host the G7 Future Tech Forum in September 2021 convening representatives of governments, industry, academia and other key stakeholders to discuss regulatory strategies for online safety.

The G20 Digital Economy Task Force has developed a Repository of Digital Policies covering skills for the future of work, digital inclusion, digital infrastructure, emerging technologies, digital government and small company entrepreneurship.[8] It seems focused on compiling a library of policies and initiatives in the G20 countries related to economic development rather than on direct dialogue among regulators. It has not yet turned to online safety and transparency issues, but its more extensive country membership might provide an opportunity for broader sharing of digital regulatory experiences and knowledge.

Intergovernmental organizations provide another avenue for regulatory cooperation. The International Telecommunication Union and the World Bank have joined forces to create a digital regulation platform. This is a library of studies on regulatory strategies, best practices and case studies related to the digital economy and might provide an outlet for spreading ideas and experiences developed in the course of digital regulation. It has not yet developed into a forum for digital regulators to meet and share experiences.

The OECD has several initiatives under way related to regulatory cooperation. Australia, New Zealand and the OECD started a project in 2019 to develop voluntary transparency reporting protocols on preventing, detecting and removing terrorist and violent extremist content from online platforms. This ongoing project aims to develop clear measures of success that will establish a global level-playing field, avoid regulatory fragmentation and reduce reporting burdens for online companies. In addition, the OECD has separately urged online platforms to issue monthly transparency reports on the prevalence of COVID-19 disinformation on their systems and has suggested that the OECD would be an ideal forum for coordination on a common reporting standard. A final relevant OECD initiative is its global partnership on AI that links

[8] See https://assets.innovazione.gov.it/1628073696-g20detfoecdcompendiumdigitaltools.pdf.

its member countries and other stakeholders in an international effort to promote responsible AI use.

A final avenue for international coordination would be through the convening power of non-governmental organizations (NGOs). CIGI operates the GPGN, a forum of digital regulators, civil servants and legislative staff developing new online regulatory institutions and frameworks. The meetings of its Transparency Working Group provided the basis for this report. This network could easily develop into an ongoing institution to share best practices and experiences in online safety regulation, including standards for transparency reports.

Other NGOs could also create a venue for a digital regulatory cooperation forum. The Institute for Strategic Dialogue operates a Digital Policy Lab that brings together digital regulators and civil servants to foster intergovernmental exchange on regulation of disinformation, hate speech, extremism and terrorism online. The Brookings Institution's Forum on International Cooperation on AI brings together officials from Australia, Canada, the European Union, Japan, Singapore and the United States on AI issues.

The World Economic Forum has organized a public-private partnership for cooperation, the Global Coalition for Digital Safety, to tackle harmful content online, which could serve as a network to exchange best practices for new online safety regulation.[9] This coalition is broader than the regulatory community, with representatives from digital companies, universities, think tanks and other NGOs as well as digital regulators. The Carnegie Endowment for International Peace has organized the Partnership for Countering Influence Operations, a community of academics, social platforms, think tanks and governments focused on research to control online disinformation.[10] Its Survey on Data-Sharing & Evidence-Based Policy to Counter Influence Operations is one tool in this effort to gather and disseminate best practices.[11]

Conclusion

Policy makers in many jurisdictions have concluded that social media companies have too much unchecked power and are failing to protect the public and their users from online harms. They are prepared to move forward with an ambitious reform agenda that includes focusing competition policy specifically on tech companies and addressing online safety issues. In many ways, transparency measures are low-hanging fruit in this new digital regulatory scheme, an area where different countries might agree even if they disagree on more controversial topics such as the mandated removal of harmful but legal material. These measures provide due process protections for users, motivate companies to do a better job of content moderation, allow shared knowledge on effective techniques to counteract harmful or illegal online material, measure compliance with regulatory requirements and provide feedback for regulators seeking to improve their regulatory programs.

There is a rich set of examples across countries and digital platforms to draw on, including pending measures to regulate digital companies in Australia, the European Union, Canada, Ireland, the United Kingdom and the United States. As transparency requirements are set, it is important to ensure that they are not dominated by the regulated companies themselves or by other vested interests and that they are developed in a multi-stakeholder and representative manner.

This conference report has surveyed some of the issues that policy makers will have to grapple with as they move forward with transparency measures, and at the same time has provided some guidance on how policy makers in several jurisdictions have addressed these implementation issues. No innovative regulatory regime can be perfect from the start; inevitably, a new regime is a work in progress that will have to be adjusted as experience is gathered. This report is intended to be a contribution to the ongoing conversation of how to set up a flexible, agile regulatory regime that can learn from experience and respond to the evolving business and technological realities of the fast-changing digital landscape.

[9] See www.weforum.org/global-coalition-for-digital-safety/home.

[10] See https://carnegieendowment.org/specialprojects/counteringinfluenceoperations.

[11] See https://survey.alchemer.com/s3/6424040/Partnership-for-Countering-Influence-Operations-Data-Sharing-Evidence-Based-Policy-Survey.

Appendix 1

Table 1: Type of Information Disclosed by Category of Recipient — Sample Policy Choices

Information Type	Terms and Conditions	User	Public Report/ Database	Auditor	Vetted Researcher	Regulator
Content moderation program						
Content rules	√					
Enforcement procedures	√					
Complaint process	√					
Misuse policy	√					
Misuse warnings		√				
Explanations		√				
Redress rights	√	√				
Trusted flaggers			√			
Operation of program			√	√	√	√
Algorithms — main parameters	√	√				
Algorithms — technical detail				√	√	√
Advertising						
Content		√	√			
Sponsorship		√	√			
Total and targeted audience			√			
Main targeting criteria		√	√			
Algorithms — technical detail				√	√	√
Operation of service						
Average monthly users			√			√
Monitoring and compliance data				√	√	√
Recommendation algorithms				√	√	√
Commercially sensitive data				√	√	√
Systemic risks					√	√
Personal data						√

Appendix 2

Resources and References

Australia

Parliament of Australia, "Online Safety Bill 2021," www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6680.

Australian Government, eSafety Commissioner, "Our legislative functions," www.esafety.gov.au/about-us/who-we-are/our-legislative-functions; "Safety by Design," www.esafety.gov.au/about-us/safety-by-design.

Parliament of Australia, "News Media and Digital Platforms Mandatory Bargaining Code," Bill 2020, https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6652_first-reps/toc_pdf/20177b01.pdf.

Canada

Government of Canada, Department of Justice, "Combatting hate speech and hate crimes: Proposed legislative changes to the Canadian Human Rights Act and the Criminal Code," June 23, 2021, www.justice.gc.ca/eng/csj-sjc/pl/chshc-lcdch/index.html.

Government of Canada, Department of Canadian Heritage, "The Government's proposed approach to address harmful content online," July 29, 2021, www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html.

Government of Canada, Department of Canadian Heritage, "Proposal to Modernize the Broadcasting Act (Bill C-10)," November 3, 2020, www.canada.ca/en/canadian-heritage/services/modernization-broadcasting-act.html; most recent text, June 21, 2021, https://parl.ca/DocumentViewer/en/43-2/bill/C-10/third-reading.

European Commission

European Commission, "The Digital Services Act: ensuring a safe and accountable online environment," December 15, 2020, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.

European Commission, "The Digital Markets Act: ensuring fair and open digital markets," December 15, 2020, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

European Commission, "Code of Practice on Disinformation," September 2018, https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation; "Guidance on Strengthening the Code of Practice on Disinformation," May 26, 2021, https://digital-strategy.ec.europa.eu/en/library/guidance-strengthening-code-practice-disinformation.

European Union, "Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online," https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0784&from=EN.

European Commission, "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts," April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.

Germany

Germany, Network Enforcement Act of 2017 (NetzDG), English Translation, German Law Archive, https://germanlawarchive.iuscomp.org/?p=1245.

Ireland

Republic of Ireland, Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, "Online Safety and Media Regulation Bill," Updated June 2, 2021, www.gov.ie/en/publication/d8e4c-online-safety-and-media-regulation-bill/#.

Republic of Ireland, BAI, "BAI publishes submission on regulation of harmful online content / implementation of new Audiovisual Media Services Directive," June 24, 2021, www.bai.ie/en/bai-publishes-submission-on-regulation-of-harmful-online-content-implementation-of-new-audiovisual-media-services-directive/.

United Kingdom

United Kingdom, Department for Digital, Culture, Media & Sport, "G7 Digital and Technology — Ministerial Declaration," April 28, 2021, www.gov.uk/government/publications/g7-digital-and-technology-ministerial-declaration.

United Kingdom, Department for Digital, Culture, Media & Sport, G7 Digital and Technology Track, "G7 Internet Safety Principles," April 28, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986161/Annex_3__Internet_Safety_Principles.pdf.

United Kingdom, Department for Digital, Culture, Media & Sport, "Draft Online Safety Bill," May 12, 2021, www.gov.uk/government/publications/draft-online-safety-bill.

United Kingdom, Department for Digital, Culture, Media & Sport and Department for Business, Energy and Industrial Strategy, "A new pro-competition regime for digital markets," July 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1003913/Digital_Competition_Consultation_v2.pdf.

PA Consulting Group, "Transparency in the Regulation of Online Safety Research Report for Ofcom," May 2021, www.ofcom.org.uk/__data/assets/pdf_file/0020/220448/transparency-in-online-safety.pdf.

United Kingdom, Competition and Markets Authority, "The Digital Regulation Cooperation Forum," March 10, 2021, www.gov.uk/government/collections/the-digital-regulation-cooperation-forum

United States

US Congress, Draft US legislation, S. 797 — The Platform Accountability and Transparency Act of 2021, introduced by US Senator Brian Schatz, March 17, 2021, www.congress.gov/117/bills/s797/BILLS-117s797is.pdf.

Lori Trahan (US Congress), Social Media Disclosure and Transparency of Advertisements (DATA) Act, February 2021, https://trahan.house.gov/uploadedfiles/social_media_data_act_bill_text.pdf.

US Financial Industry Regulatory Authority (FINRA), www.finra.org/#/.

Seila Law LLC v. Consumer Financial Protection Bureau, No. 19-7, June 29, 2020, www.supremecourt.gov/opinions/19pdf/19-7_n6io.pdf..

OECD

OECD, "G20 Compendium on the Use of Digital Tools for Public Service Continuity," Report for the G20 Digital Economy Task Force, https://assets.innovazione.gov.it/1628073696-g20detfoecdcompendiumdigitaltools.pdf.

OECD, "Trans-governmental networks," www.oecd.org/gov/regulatory-policy/irc7.htm.

OECD, "The International Regulatory Co-operation Toolkit," www.oecd.org/gov/regulatory-policy/irc-toolkit.htm.

OECD, "Combatting COVID-19 disinformation on online platforms," July 3, 2020, www.oecd.org/coronavirus/policy-responses/combatting-covid-19-disinformation-on-online-platforms-d854ec48/.

OECD, "The Global Partnership on AI," https://gpai.ai.

Independent Research Institutions

Institute for Strategic Dialogue, "Digital Policy Lab," www.isdglobal.org/digital-policy-lab/.

World Economic Forum, "Global Coalition for Digital Safety," www.weforum.org/global-coalition-for-digital-safety/home.

Carnegie Endowment for International Peace, "Partnership for Countering Influence Operations," https://carnegieendowment.org/specialprojects/counteringinfluenceoperations.

Carnegie Endowment for International Peace, "Survey on Data-Sharing & Evidence-Based Policy to Counter Influence Operations," https://survey.alchemer.com/s3/6424040/Partnership-for-Countering-Influence-Operations-Data-Sharing-Evidence-Based-Policy-Survey.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org