CENTER FOR DEMOCRACY & TECHNOLOGY

Comments of the Center for Democracy & Technology

To the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression in the consultation on 'Freedom of expression and the private sector in the digital age'

29 January 2016

The Center for Democracy & Technology welcomes this opportunity to provide input for the report that the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression, David Kaye, is preparing on the relationship between freedom of expression and the private sector in the digital age. Below, we provide information and resources about two emerging areas of focus in this topic: the role of financial intermediaries, and the use by governments of companies' privately developed content policies or Terms of Service to seek the removal of online content.

I. Categories of actors in the ICT sector whose activities implicate the freedom of opinion and expression: Financial Intermediaries

The global Internet has become an indispensable medium for the freedom of expression. Billions of people around the world use the Internet to exchange ideas and information; gather and disseminate news and research; discuss and debate social and economic policy; create, share, and preserve art and literature; purchase goods and services; conduct business; contact loved ones and meet new people; organize their lives and record their private thoughts. Out of technical necessity, all of this online expression relies on the use of the equipment and services of a series of third-party intermediaries.[1]

Internet users depend on the interconnected network of technical intermediaries, including backbone network operators, Internet service providers (ISPs) and telecommunications carriers, content delivery networks, and remote hosting providers to exchange and store data. They also rely on the millions of websites, online services, and applications that run on this infrastructure to access forums for searching for and sharing information and ideas, and for connecting with other Internet users around the world.[2] The role of these primarily private-sector technical intermediaries in facilitating individuals' freedom of expression online has been well documented by a number of expert commentators, including in previous reports from the Special Rapporteur on freedom of opinion and

[1] For an overview of technical intermediaries, see Center for Democracy & Technology, Shielding the Messengers: Protecting Platforms for Expression and Innovation (2012) *available at* https://cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf.

[2] Online service providers, including blog platforms, email service providers, social networking websites, and video and photo hosting sites, provide access to user-generated content or allow user-to-user communications.

expression.[3] A recent report from UNESCO provides a comprehensive review of the many forms and functions of intermediaries in the Internet ecosystem and discusses the way these entities enable freedom of expression for Internet users around the world.[4]

But individuals' access to the expressive ecosystem of the Internet is contingent on a number of other intermediary actors, again primarily operating in the private sector. A prime example of this is the category of financial intermediaries – the credit card companies, banks, and third-party payment processors that enable individual speakers and website operators to engage in financial transactions. Website operators use financial service providers such as credit cards to buy domain names and rent server space for their speech, to purchase Internet access services, and to pay their staff. A website operator whose bank or credit card account is cut off loses the ability to complete those transactions that are necessary to keep his or her site online.[5] The structure of the credit card industry, in particular – which is concentrated in two major payment systems, Visa and MasterCard, accounting for nearly 80 percent of online transactions – make these payment systems key intermediaries enabling and supporting online content.[6]

Because of financial intermediaries' emerging role as 'gatekeepers' for online expression, these intermediaries are an increasingly attractive target of government or private censors who cannot – for legal, political, or jurisdictional reasons – directly suppress the speech they wish to be silenced. Financial intermediaries may make a particularly attractive target for this type of pressure, since they are often further removed from the speech interests at stake, or are more vulnerable to the prospect of reputational harm, than application-layer intermediaries such as content platforms and hosts. Several high-profile examples from the United States highlight the vulnerability of expressive freedoms to proxy censorship via financial intermediaries, underscoring censorship pressures on advertisers and

---

[3] *See, e.g.,* Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations General Assembly document A/66/290 (16 May 2011), *available at* http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

[4] See UNESCO, Fostering Freedom Online: The Role of Internet Intermediaries (2014), *available at* http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.

[5] An operator who is cut off from financial services also loses the ability to receive payments from ad networks and direct advertisers for hosting advertising on his or her site. CDT discussed this issue in depth in our amicus brief in *Backpage v. Dart,* No. 15-3047 (7th Cir. Nov. 30, 2015), slip op. *available at* http://media.ca7.uscourts.gov/cgi-bin/rssExec.pl?Submit=Display&Path=Y2015/D11-30/C:15-3047:J:Posner:aut:T:fnOp:N:1663542:S:0. *See Amicus* brief of Center for Democracy & Technology et al, *available at* https://cdt.org/files/2015/11/Backpage.com-v.-Dart-7th-Circuit-amicus-brief-CDT-EFF-AAN-FINAL.pdf. But even subscription-based news site that cannot make electronic payments will be unable to continue publishing online. A newspaper with a website such as The Washington Post must pay an ISP to provide the service of connecting to the Internet in order to transmit its stories to subscribers and other readers. The Washington Post must pay a domain name registrar, such as MarkMonitor, Inc., to obtain its domain name (https://www.washingtonpost.com), and it must purchase and maintain its own servers or transact with a website hosting company that rents server space to host the site and its ever-changing content.

[6] *See* Annemarie Bridy, *Internet Payment Blockades* at 4, 67 Fla. L. Rev. 1523 (Sept. 2015), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2494019.

payment processors as a free expression issue.[7] However, the nature, extent and impact of such censorship pressures on financial intermediaries remain an underexplored legal and policy issue.

II. Main legal issues raised for freedom of opinion and expression within the ICT sector: Internet Referral Units

The pressures facing technical intermediaries from actors in government and the private sector are well documented: Internet intermediaries are pushed to control or police user content and activity in a wide range of circumstances, including in response to claims of defamation, obscenity, intellectual property infringement, invasion of privacy, or because content is critical of the government.[8] But increasingly, governments are engaged in a different kind of extralegal censorship via intermediaries, in the form of leveraging companies' privately developed Terms of Service (TOS) enforcement mechanisms to seek removal of content that may not violate national law.

These programs are already underway in a number of states. For example, several years ago the UK government created the Counter-Terrorism Internet Referral Unit (CTIRU), a unit within the police force that seeks to remove 'extremist' content from the web by, among other methods, using websites' content-flagging mechanisms to report content as a violation of the site's TOS.[9] The CTIRU

---

[7] For example, in the United States in 2012, WikiLeaks revealed that U.S. Congressmen Joseph Lieberman and Peter King had pressured MasterCard and possibly Visa to stop processing payments to the anti-secrecy organization. *See* Michael Tennant, *Documents Show Lieberman, King Behind Financial Blockade of WikiLeaks*, New American (Nov. 28, 2012), http://www.thenewamerican.com/usnews/congress/item/13762-documents-show-lieberman-king-behind-financial-blockade-of-wikileaks. Senator Lieberman also reportedly pressured Amazon.com, publicly and privately, to terminate its hosting services for WikiLeaks. Ewen MacAskill, *WikiLeaks Website Pulled by Amazon After US Political Pressure*, Guardian (Dec. 1, 2010), http://www.guardian.co.uk/media/2010/dec/01/wikileaks-website-cables-servers-amazon. Ultimately, most of the major banks, credit card networks, and money transfer companies, including Bank of America, Visa, MasterCard, Western Union, and PayPal, discontinued service to WikiLeaks, cutting it off from 95 percent of its revenues from donations. John P. Mello, *WikiLeaks Suspends Publication Because of Financial Boycott*, PCWorld (Dec. 7, 2010), http://www.pcworld.com/article/242470/wikileaks_suspends_publication_because_of_financial_boycott.html. WikiLeaks stopped publishing and went offline for months while it sought to raise funds through alternative channels.

In 2015, an Illinois sheriff intent on shutting down the popular classified ads site Backpage.com sent letters addressed to the CEOs, Board of Directors, and top institutional investors of Visa and MasterCard, Backpage's primary financial services providers. These letters demanded that the card companies 'cease and desist' from their business relations with the site and implied that they could face civil or criminal liability for continuing to process payments for ads linked to unlawful activity. *See* Backpage.com v. Dart, *supra* n.5. The letters invoked the reputational damage that the credit card companies would face if they continued to provide service to Backpage.com, and Sheriff Dart followed up these missives with phone calls and emails that promised to single out the card companies in press conferences if they did not cooperate. Within 48 hours, both MasterCard and Visa had terminated Backpage's accounts.

[8] *See, e.g.*, Jack M. Balkin, *Old School/New School Speech Regulations*, 127 Harv. L. Rev. 2296 (2014), *available at* http://ssrn.com/abstract=2377526; Derek E. Bambauer, *Against Jawboning*, 100 Minn. L. Rev. 51 (2015), *available at* SSRN: http://ssrn.com/abstract=2581705.

[9] *See* National Police Chiefs' Council, The Counter Terrorism Internet Referral Unit at 3, http://www.npcc.police.uk/NPCCBusinessAreas/PREVENT/TheCounterTerrorismInternetReferralUnit.aspx (last visited Jan. 28, 2016).

has achieved removal of 4,000 pieces of content a month in 2015, 'taking the total to 110,000 pieces of propaganda removed' since 2010.[10] In July 2015, Europol launched an EU-wide version of this program,[11] on the recommendation of the EU Counter-Terrorism Coordinator, who noted that 'platforms' own terms and conditions . . . often go further than national legislation and can therefore help to reduce the amount of radicalising material available online.'[12] And in January 2016, the U.S. government called for a meeting of major Internet companies for which a government 'flagging' proposal appeared at the top of the agenda.[13]

This type of government-initiated content flagging program raises a number of challenges under the human rights framework. Companies' privately developed Terms of Service and content policies are typically more restrictive, and often much more restrictive, than what governments may permissibly restrict under law. Further, these programs may not be clearly articulated in law; the specific procedures and processes are often not communicated transparently with the public, and there has not been an evidence-based showing that they are necessary or effective. Finally, they are not susceptible to normal processes of democratic governance and oversight. Overzealous efforts to pursue expedited, privatized removal of content risk undermining the rule of law and fundamental values of a democratic society.

Internet referral unit programs permit governments to seek the removal of content that they would not necessarily be permitted to censor under international human rights law. When Internet companies create their TOS, they consider a wide variety of factors that go well beyond merely what is impermissible under the law. Operators of websites and social networks develop policies based on the type of user-base and community they are seeking to attract and the subject matter of the site. A blog devoted to baking might prohibit any discussion of politics or current events in its TOS, to keep commenters on-topic – a reasonable response for a website operator, but something the government could not do.

---

[10] Home Office, Counter-Extremism Strategy, Command Paper (Cm 9148) at 24 (presented to Parliament Oct. 19, 2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/470088/51859_Cm9148_Accessible.pdf.

[11] Europol, Europols Internet Referral Unit to Combat Terrorist and Violent Extremist Propaganda (July 1, 2015), https://www.europol.europa.eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda.

[12] Memorandum from the EU Counter-Terrorism Coordinator to Delegation of Standing Committee on Operational Cooperation on Internal Security (COSI) Re: EU CTC Input for the Preparation of the Informal Meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015 (Jan. 20, 2015), *available at* http://www.statewatch.org/news/2015/jan/eu-council-ct-ds-1035-15.pdf (last visited Jan. 28, 2016).

[13] Memorandum Re: White House Briefing Document for Jan. 12 Counterterrorism Summit With Tech Leaders (undated), *available at* https://theintercept.com/document/2016/01/20/white-house-briefing-document-for-jan-12-counterterrorism-summit-with-tech-leaders/ (last visited Jan. 28, 2016).

In seeking content removal through TOS enforcement, the government actor is relying on companies' definitions of terms such as threats,[14] violent or graphic content,[15] malicious speech,[16] and 'dangerous organizations',[17] rather than content that may be prohibited or punished in accordance with international human rights law. There may be no restrictions against the government flagging the documentation of human rights violations that involve depictions of violence, political or religious speech that appears to meet a company's definition of harassment, or controversial but lawful associations. Even the most clearly articulated or narrowly drawn of companies' content policies will tend to go well beyond what government may permissibly censor, and these policies exist as privately developed codes of conduct, not publicly promulgated regulations that can be challenged in court. Further, a government official seeking to restrict content through a company's TOS is seeking removal of that content worldwide, exceeding the scope of that official's jurisdiction.

Governments have an affirmative obligation under international human rights law to ensure that policies are articulated in law and are based in evidence that they are likely to achieve the compelling goal or interest of the state. IRUs fail in these respects because they create a risk of arbitrary and overbroad enforcement that has not been demonstrated to achieve the legitimate ends of the state, and deny individuals procedural safeguards against improper government censorship of their expressive activities. IRU programs allow government officials to seek content restriction with no review by a judge or other independent authority, thus circumventing key procedural protections for individuals' freedom of expression. Individuals whose expression is affected by these state-run programs have no opportunity to seek redress against the government. They have no notice that a government agent was involved in flagging their expression, and no remedy for or opportunity to appeal a mistaken removal of their protected expression at the behest of their government.[18] Governments seeking removal of unlawful content must do so by procedures that are provided by law,

---

[14] Twitter Support, https://support.twitter.com/articles/18311 (last visited Jan. 28, 2016).

[15] YouTube Help, Violent or Graphic Content, https://support.google.com/youtube/answer/2802008 (last visited Jan. 28, 2016).

[16] Tumblr Policy, Community Guidelines (last modified Jan. 26, 2015), https://www.tumblr.com/policy/en/community (last visited Jan. 28, 2016).

[17] Facebook, Community Standards, https://www.facebook.com/communitystandards (last visited Jan. 28, 2016).

[18] No company has a perfect record on content removal, even according to their own Terms of Service. Every company's review and moderation processes will be vulnerable to error – this is simply inevitable at the scale at which they operate. On the one hand, because no process is perfect, content that could or should be removed under a company's Terms of Service may be missed, and not removed. If companies face potential legal sanction for failure to remove content, this type of potential error leads to over-blocking of protected speech. This risk is why we have seen wide recognition of the importance of legal protections from intermediary liability for free expression online, including in reports of the current and former Special Rapporteurs on Free Expression, as well as in UNESCO's Internet Study from earlier this year. United Nations Educational, Scientific and Cultural Organization (UNESCO), Keystones to Foster Inclusive Knowledge Societies: Access to Information and Knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet (2015), http://unesdoc.unesco.org/images/0023/002325/232563E.pdf. On the other hand, the error may be a false-positive and content that does not violate Terms of Service, much less the law, is removed. This scenario raises a number of questions: What is the remedy for the speaker who has been silenced, and against whom? What else happens to this speaker and her personal information, if she is erroneously identified by or to the government as being associated with 'extremist' speech or online terrorist activity?

and that ensure accountability and an opportunity for appeal. Such restrictions must be the least restrictive and proportionate means to achieve the government's aim. IRUs are not amenable to and may in many cases be incompatible with these requirements.

Vague and overbroad policies that shift too much responsibility onto private companies and remove procedural protections for fundamental rights threaten the existence of liberal democracies founded on the ideals of freedom of expression and opinion. Government use of privately developed content moderation systems to seek removal of 'extremist' content is precisely this sort of policy, and raises significant questions about the role of the private sector, and of governments, in fostering freedom of expression in the digital age. We urge the Special Rapporteur to examine this topic in his future reports.

* * *

Thank you for the opportunity to contribute to this important report. We look forward to future engagement with the Special Rapporteur on these topics.

Sincerely,

Emma J. Llansó
Director, Free Expression Project

Rita Cant
Free Expression Fellow
Center for Democracy & Technology