July 17, 2018

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW., Room 4725,
Washington, DC 20230

Via email: iipp2018@ntia.doc.gov

Attn: Fiona Alexander

Re: International Internet Policy Priorities (Docket No. 180124068-8068-01)

The Center for Democracy & Technology (CDT) respectfully submits these comments to the National Telecommunications and Information Administration (NTIA) in its inquiry on international internet policy priorities. CDT is a non-profit public interest advocacy organization that works to promote individual rights in internet law and policy in the United States and around the world.

Protecting fundamental rights goes hand-in-hand with promoting ethical innovation and sustainable growth of the internet economy. Below, we discuss a variety of trends and issues that feature prominently in international internet-related policy debates and provide resources and recommendations for NTIA priorities. We specifically focus on content moderation, Internet of Things, global privacy rules, cybersecurity and cross border data flows.

Pressures around online content moderation threaten the free flow of information and jeopardize the limitations on liability for internet intermediaries that have proven to be a cornerstone for both free expression and innovation online. As many governments, including some of the United States' closest allies and trading partners, demand faster and more comprehensive monitoring of online speech for potential illegal activity, there is a significant risk of distorting the online information environment and suppressing lawful speech. Concern about challenging issues such as disinformation, terrorist propaganda, and hate speech are driving both industry self-regulation and legislative activity around the world. NTIA has an important role to play in bilateral, regional, and global fora to call for sound, evidence-based approaches to policymaking that account for the risk of unintended consequences for the economy and society.

The NTIA has also solicited comments on trends in emerging technologies and how best to engage in international discussions around privacy and cybersecurity. We suggest, first, that the NTIA build on its expertise in the commercial Internet of Things (IoT) to encourage better data practices and consideration of security and safety in connected devices around the globe.

Consumers, international and domestic, are concerned about "unsafe" IoT and systemic problems in the IoT ecosystem pose a global threat. Second, we would encourage the Department of Commerce to advance new thinking on how to harmonize U.S. privacy laws with emerging global data protection norms, emphasizing the overarching role that transparency, control, and individual autonomy should play in any privacy framework.

In considering cybersecurity, we recommend the NTIA prioritize encouraging companies to adopt strong encryption practices and work with the international community to set norms that permit encryption to be adopted and preserved. Encryption allows millions of Americans to safely use the internet everyday, which has enabled the internet to become a valuable sector for the US economy. Law enforcement demands for backdoor access, or weakening encryption standards put all of this at jeopardy. Furthermore, as the internet is further integrated into people's lives and commerce, software vulnerabilities carry increasing risk and cost to people, businesses and the economy. Government actors that identify software vulnerabilities must determine whether or not to reveal them or to exploit them for national security purposes. The U.S. government recently released a Vulnerabilities Equities Process charter which transparently and thoughtfully informs the public how the government approaches these decisions. NTIA should work with its foreign counterparts to create transparent, thoughtful vulnerabilities equities processes of their own.

Finally we urge the NTIA to assume a monitoring role with respect to the agreements made in accordance with the CLOUD ACT. The legislation fails to adequately ensure that human rights are protected in cross-border data demands. It is also unclear if the U.S. Department of Justice will apply its policy of using a warrant for content to foreigners. If not, this would call into question the ability of U.S. providers to adequately protect content of foreign companies and persons against unfounded demands for it from the U.S. government and would put U.S. providers at a competitive disadvantage. It is vital that NTIA voice these concerns.

I. The Free Flow of Information and Jurisdiction

1. Changing Intermediary Liability Frameworks Threaten the Free Flow of Information Online.

The history of the internet to date demonstrates that the policy framework protecting intermediaries from liability for the acts of their users is necessary to support the free flow of information online. The US internet industry is a global leader precisely because of the protections afforded intermediaries by Section 230 of the Communications Decency Act and

Section 512 of the Digital Millennium Copyright Act,[1] and the importance of limiting intermediary liability for the promotion of free expression online is widely recognized.[2]

Increasingly, however, legal frameworks that limit liability for internet intermediaries are under threat—both domestically and internationally. Governments around the world are pressuring intermediaries, particularly content hosts, to take a more active role in policing user-generated content. This pressure is typically accompanied by threats to rescind liability limitations and to create new legal obligations to monitor and evaluate individuals' speech in extremely tight time frames.

For example, under the recent *NetzDG* law in Germany, social media companies and other providers that host third-party content face fines of up to €50 million if regulators find systematic failures in their processes for evaluating and removing "obviously illegal" speech within 24 hours of it being flagged by users or other individuals.[3] The European Commission's (EC) Code of Conduct on Countering Illegal Hate Speech Online, signed by Facebook, Microsoft, Twitter and YouTube in May 2016, commits companies to review notifications of illegal hate speech within 24 hours.[4] The EC's "Recommendation on measures to effectively tackle illegal content online" suggests several methods for hosts of user-generated content to address allegedly illegal speech more quickly, including "trusted flaggers," Internet Referral Units, and shared hash databases.[5]

Crucially, none of these methods involve adjudication of individuals' speech by an independent judge and instead put private companies in the position of evaluating whether content violates national law. This is an inappropriate role for private companies to play, as it circumvents the role of the judiciary in a rule-of-law system and can interfere with an individual's ability to hold the government accountable for deeming his speech 'illegal'.

---

[1] CENTER FOR DEMOCRACY & TECHNOLOGY, SHIELDING THE MESSENGERS: PROTECTING PLATFORMS FOR EXPRESSION AND INNOVATION 4-5 (2d ed. 2012), https://cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf [hereinafter SHIELDING THE MESSENGERS].

[2] *See, e.g.,* United Nations, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/17/27, 2011, http://www2.ohchr.org/english/bodies/hrcouncil/17session/reports.htm; Manila Principles on Intermediary Liability, 2015, https://www.manilaprinciples.org/.

[3] Center for Democracy & Technology, The Netzwerkdurchsetzungsgesetz (NetzDG) Network Enforcement Law, https://cdt.org/files/2017/07/NetzDG-Law-Overview.pdf [hereinafter "NetzDG Overview"]. *See also* Emma Llansó, *German Proposal Threatens Censorship on Wide Array of Online Services*, CTR. FOR DEMOCRACY & TECH. (April 7, 2017), https://cdt.org/blog/german-proposal-threatens-censorship-on-wide-array-of-online-services.

[4] Jens-Henrik Jepessen, *First Report on the Hate Speech Code of Conduct shows need for transparency, judicial oversight, and appeals,* CTR. FOR DEMOCRACY & TECH. (Dec. 12, 2016), https://cdt.org/blog/first-report-eu-hate-speech-code-of-conduct-shows-need-transparency-judicial-oversight-appeals [hereinafter *First Report*].

[5] Emma Llansó, *Who Needs Courts? A Deeper Look At The European Commission's Plans to Speed Up Content Takedowns*, CTR. FOR DEMOCRACY & TECH. (Mar. 1, 2018), https://cdt.org/blog/who-needs-courts-a-deeper-look-at-the-european-commissions-plans-to-speed-up-content-takedowns [hereinafter *Who Needs Courts?*].

Such methods are also highly likely to lead to overbroad censorship.[6] For intermediaries, a cost-benefit analysis almost always militates in favor of removing content. The benefit of keeping any individual post on a platform is minimal compared to the risk of incurring liability for failing to remove content ultimately found to be illegal. Absent strong protections against liability, incentives skew strongly in favor of intermediaries removing material as soon they receive a request to do so—even if the request comes from a private party rather than a court.[7] These methods of notifying intermediaries of allegedly illegal speech on their services typically lack safeguards for users on two levels: (1) ensuring that the notice procedure is not abused by malicious private actors,[8] and (2) allowing appeals for users whose lawful content is taken down.[9]

There is also a lack of transparency about both government requests for removal and intermediaries' removal decisions, which could provide high-level safeguards against systemic threats to free expression.[10] To be valuable, though, disclosure must go beyond naïve reliance on blunt, easily quantifiable metrics such as content takedown rate, as it is not clear whether an increasing takedown rate is normatively desirable from a policy perspective.[11] An increasing takedown rate could, for instance, indicate an increased removal of illegal content or simply an increase in false positives (i.e., increased removal of legal content). Separating signal from noise depends on an analysis of the context of each takedown request.[12]

---

[6] Emma Llansó, Center for Democracy & Technology, Comments to the EC on tackling illegal content online (Mar. 29, 2018), http://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-1183598/feedback/F10987_en [hereinafter "Comments to the EC"].

[7] SHIELDING THE MESSENGERS, *supra* note 1, at 10. *See also* Liz Woolery, Center for Democracy & Technology, Comments to UNESCO, https://en.unesco.org/sites/default/files/ui_c2_en_sub092.pdf **(**Describing how the Copyright Directive incentivizes intermediaries to "play it safe" in removing content that has any chance of being illegal).

[8] Jens-Henrik Jeppesen & Emma Llansó, Center for Democracy & Technology, Letter to Commissioner Věra Jourová of the E.C. (June 3, 2016), https://cdt.org/files/2016/06/CDT-letter-to-Commissioner-Jourova-on-hate-speech-Code-of-Conduct.pdf (highlighting that the proposed Hate Speech Code of Conduct includes no safeguards against misuse of the notice procedure, even though it is well understood that a notice-and-takedown regime can be vulnerable to abuse by those seeking to silence diverse views).

[9] Emma Llansó & Rita Cant, Center for Democracy & Technology, Comments to UN Special Rapporteur David Kaye (Jan. 29, 2016), https://cdt.org/files/2016/02/CDT-Comments-Consultation-on-freedom-of-expression-and-the-private-sector-in-the-digital-age.pdf (describing how Internet Referral Units provide users "no remedy for or opportunity to appeal a mistaken removal of their protected expression at the behest of their government.").

[10] U.N., Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶ 9, U.N. Doc. A/HRC/38/35 (April 6, 2018), https://freedex.org/a-human-rights-approach-to-platform-content-regulation [hereinafter "Report of UN Special Rapporteur"] ("Companies do not consistently disclose sufficient information about how they respond to government requests, nor do they regularly report government requests made under terms of service.")

[11] Letter to Commissioner Věra Jourová of the E.C., *supra* note 17 ("The metric for success cannot just be the quantity of content detected and removed.").

[12] Emma Llansó, *German Social Media Law Creates Strong Incentives for Censorship*, CTR. FOR DEMOCRACY & TECH. (July 7, 2017), https://cdt.org/blog/german-social-media-law-creates-strong-incentives-for-censorship.

Finally, there is also an increasing trend towards mandates for persistent monitoring to ensure that removed content does not reappear.[13] (We discuss the risks of automated content analysis to the free flow of information in more detail below.) Content moderation or monitoring requirements and uncertainty over future regulations both increase platform compliance costs, which in turn raises industry barriers to entry and threatens to entrench dominant players.[14]

RECOMMENDATION: Through its role in trade negotiations and participation in inter-governmental fora, the Department of Commerce should work with its counterparts in other countries to emphasize the importance of intermediary liability protections in global commerce, and to promote similar policies abroad. Judges should decide whether content violates the law, initiatives to address illegal content should be narrowly tailored and proportionate to a legitimate aim, and users should retain access to procedural safeguards such as notice and appeal.

2. Increasing Voluntary and Mandated Use of Automated Content Monitoring and Filtering Poses a Particular Threat to the Free Flow of Information Online.

a. Regulators Have Repeatedly Called for Faster Content Moderation by Internet Platforms to Respond to a Variety of Policy Problems.

Regulators increasingly pressure platforms to moderate lots of content, and to do so quickly. For example, *NetzDG* and the Hate Speech Code of Conduct mandate the removal within 24 hours of manifestly illegal content and illegal hate speech, respectively.[15] There are also

---

[13] Jens-Henrik Jeppesen & Laura Blanco, *Tackling 'Illegal' Content Online: The EC Continues Push for Privatised Law Enforcement*, CTR. FOR DEMOCRACY & TECH. (Oct. 3, 2017), https://cdt.org/blog/tackling-illegal-content-online-the-ec-continues-push-for-privatised-law-enforcement [hereinafter *Tackling 'Illegal' Content Online*] (discussing the de facto obligation the EC places on Internet intermediaries to monitor all content to make sure that illegal content doesn't reappear). *See also* Center for Democracy & Technology, CDT's Concerns on the European Commission's Proposal for a Directive on Copyright in the Digital Single Market (Feb. 23, 2017), https://cdt.org/files/2017/02/CDT_Concerns_EC_Proposal_Directive_on_Copyright_DSM.pdf ("Article 13 [of the E-Commerce Directive] . . . imposes what amount to a general monitoring obligation on intermediaries of any kind to employ technological measures to monitor and filter uploaded content."); Jens-Henrik Jeppesen, *Audiovisual Media Service Directive: Parliament Proposals Pose New Challenges to Free Expression,* CTR. FOR DEMOCRACY & TECH. (Oct. 18, 2016), https://cdt.org/blog/audiovisual-media-service-directive-parliament-proposals-pose-new-challenges-to-free-expression ("A serious problem that runs through several parts of the DSM [Digital Single Market] Strategy is the move to push internet companies to police and monitor their platforms for content that may violate restrictions on various types of speech, such as 'hate speech' or 'glorification of terrorism'.").

[14] SHIELDING THE MESSENGERS, *supra* note 1, at 5 ("Without Section 230, open-ended liability risks would dramatically raise entry barriers for new Internet services and applications that allow user-generated content, jeopardizing innovation in interactive media."); Center for Democracy & Technology, Comments to the United States Department of Commerce National Telecommunications and Information Administration, Docket No. 100921457-0457-01 **[**hereinafter "Comments to NTIA"**]**("When intermediaries are protected from liability for their users' content, they are freer to innovate new products and services, which often serve as additional platforms for small innovators and individual speakers").

[15] NetzDG Overview, *supra* note 2.

"repeated calls from a variety of politicians around the world for tech companies to remove terrorist speech quickly and en masse."[16] Pressure to engage in speedier content moderation inevitably pushes platforms towards automated filtering of content as opposed to human review.

Calls for automated filtering, however, hinge on the dubious premise that it will be possible to develop a technical solution to the complex challenge of distinguishing 'terrorist propaganda' or 'illegal hate speech' from lawful expression—a task that yields few black-and-white answers and which can raise significant cultural and political implications.[17] Meanwhile, the use of highly flawed automated tools for content filtering gravely threatens the free flow of information, and "inevitably results in over-censorship."[18]

b. Research Demonstrates that Automated Review Increases the Likelihood of Over-Censorship, with a Disparate Impact Falling on Already Marginalized Groups.

Empirical research documents a number of problems with machine-learning tools developed for automated content analysis.[19] Machine-learning tools function best when they are trained to perform a clearly defined task, but for content-analysis challenges, there is often no clear or consistent definition of the content targeted for filtering, such as "hate speech" or "disinformation."[20] Inter-cultural variation is at least partly to blame for the lack of consistent definitions, and the need for sensitivity to cultural context militates in favor of human review. Moreover, "off-the-shelf" automation tools may be unreliable without domain-specific training (i.e., training the algorithm on a particular group of speakers, in a particular language, on a particular platform, in a particular context).[21]

Low accuracy and inter-coder reliability of content-analysis tools counsels against their use for decisions that impact fundamental speech rights.[22] For example, accuracy rates in studies of Natural Language Processing (NLP) tools hover around 80%— 1 in 5 speakers would be treated "wrong" by these tools.[23] It is particularly difficult to train machine-learning tools to detect

[16] Comments to UNESCO, *supra* note 8.
[17] Comments to UNESCO, *supra* note 8.
[18] Sydney Li & Jamie Williams, *Despite What Zuckerberg's Testimony May Imply, AI Cannot Save Us*, ELECTRONIC FRONTIER FOUNDATION (April 11, 2018), https://www.eff.org/deeplinks/2018/04/despite-what-zuckerbergs-testimony-may-imply-ai-cannot-save-us.
[19] *See, e.g.*, CENTER FOR DEMOCRACY & TECHNOLOGY, MIXED MESSAGES? THE LIMITS OF AUTOMATED SOCIAL MEDIA CONTENT ANALYSIS 10 (2017), https://cdt.org/insight/mixed-messages-the-limits-of-automated-social-media-content-analysis [hereinafter MIXED MESSAGES] (illustrating the limitations of Natural Language Processing tools known as "text classifiers.").
[20] MIXED MESSAGES, *supra* note 48, at 5.
[21] MIXED MESSAGES, *supra* note 48, at 4.
[22] *Id.* at 5.
[23] *Id.*

comparatively rare events such as incidents of hate speech or terrorist propaganda on social media.[24]

"Accuracy" is itself a contested, subjective concept in the machine-learning literature. It can be assessed in various ways, and programmatic objectives will often influence which metrics of "success" are chosen.[25] In NLP studies, accuracy often refers to how closely a tool mirrors human determinations.[26] But accuracy alone might be too blunt of a metric for judging the usefulness of a given tool. For example, even if a tool has a high overall accuracy rate, it may still have an undesirable rate of false positives, meaning that too much lawful speech is identified as potentially problematic.[27] Note that at scale, even a miniscule percentage of false positives can result in high volumes of legitimate speech being censored.[28]

Furthermore, using agreement with human determinations as the standard for algorithmic accuracy assumes that humans largely agree amongst themselves on what constitutes problematic speech. However, the literature illustrates that inter-coder reliability on whether, for example, a social media post is hate speech or extremism is actually quite low.[29] Finally, determining whether a majority of humans agree to a classification is, by definition, imposing a majoritarian view on what hate speech or extremism is, which can fail to properly account for and respect alternative and minority views.[30]

Chief among the problems that automation presents is the potential to disproportionately harm groups that are already marginalized in a given society.[31] Algorithms learn from training data, which may itself carry bias against marginalized groups, such as gender bias and bias against non-English speakers, as well as bias against dialectal variations in language used by minority populations.[32] For example, researchers found that popular NLP tools tend to misidentify African American Vernacular English as non-English.[33]

There are numerous real-world examples of the automated filtering technologies used by internet platforms exhibiting bias against marginalized groups. For example, Google's Perspective API for ranking comment toxicity gave the phrase "I am a gay black woman" an 87%

[24] *Id.* at 18.
[25] *Id.* at 17 (explaining how the success metric for an algorithm predicting school success might be grades or student engagement, depending on the user's goals).
[26] *Id.* at 5.
[27] *Id.* at 19.
[28] *Id.* at 18 fn. IV.
[29] *Id.* at 17.
[30] *Id.* at 17-18.
[31] *Id.* at 4.
[32] *Id.*
[33] *Id.*

toxicity score.[34] A Palestinian man was held and questioned by Israeli police relying on an incorrect machine translation of his Facebook post.[35] The post said "good morning" in Arabic but was translated as "attack them" in Hebrew. A University of Washington study from 2017 found that YouTube had a higher error rate for captioning female speakers than for male speakers in videos,[36] and a second study found that YouTube had a higher error rate for captioning non-white speakers.[37] As CDT has said in a previous report: "The disparate enforcement of laws or terms of service by biased algorithms that disproportionately censor people of color, women, and other marginalized groups raises obvious civil and human rights concerns."[38]

RECOMMENDATION: Law should never mandate automated filtering of illegal content by platforms.[39] Keeping in mind that automated content can over-censor already-marginalized speakers relative to the rest of the population, governments should not use automated content analysis to make decisions affecting rights, liberties, and access to benefits of individuals or groups.[40] Automated content analysis should always be accompanied by human review.[41]

3. The Extra-Territorial Application of Content Laws Represents a Race to the Bottom, as Individual Nations Seek to Censor Online Speech Beyond Their Borders.

We also note with concern the trend of courts in individual countries ordering remedies that are global in scope.[42] For example, Google has been in a longstanding legal battle with the French data protection authority, the CNIL, over whether "right to be forgotten" requests require Google to globally delist webpages for all searches conducted worldwide on Google's services.[43] And in the 2017 case *Google v. Equustek Solutions*, in which the Canadian Supreme

---

[34] Violet Blue, *Google's Comment-Ranking System Will Be a Hit With the Alt-Right*, ENGADGET.COM (Sept. 1, 2017), https://www.engadget.com/2017/09/01/google-perspective-comment-ranking-system.

[35] Alex Hern, *Facebook Translates 'Good Morning' Into 'Attack Them', Leading to Arrest*, THE GUARDIAN (Oct. 24, 2017), https://www.theguardian.com/technology/2017/oct/24/facebook-palestine-israel-translates-good-morning-attack-them-arrest.

[36] Rachel Tatman, *Gender and Dialect Bias in YouTube's Automatic Captions*, PROC. FIRST WORKSHOP ON ETHICS IN NAT. LANGUAGE PROCESSING 53 (2017).

[37] Rachel Tatman & Conner Kasten, *Effects of Talker Dialect, Gender, Race & Accuracy on Bing Speech and YouTube Automatic Captions*, INTERSPEECH 934 (2017).

[38] MIXED MESSAGES, *supra* note 48, at 5.

[39] *Id.* at 6.

[40] *Id.*

[41] *See id.* at 7 ("Questions to Guide Policymakers' Evaluation of Automated Text Analysis Tools").

[42] Report of UN Special Rapporteur, *supra* note 19, at 7-8 ("Some States are demanding extraterritorial removal of links, websites and other content alleged to violate local law... The logic of these demands would allow censorship across borders, to the benefit of the most restrictive censors.") (footnotes omitted).

[43] Emma Llansó, *Google Appeals French Data Protection Authority's Demand to Modify Search Results Worldwide*, CTR. FOR DEMOCRACY & TECH. (May 19, 2016), https://cdt.org/blog/google-appeals-french-data-protection-authoritys-demand-to-modify-search-results-worldwide.

Court ordered Google to globally delist a webpage from its search engine.[44] In doing so, the Canadian court effectively censored information for citizens of every nation in the world according to a decision based on Canadian law. However, the majority in *Equustek* brushed aside international comity concerns, calling them "theoretical."[45]

The *Equustek* decision is troubling on a number of fronts. First, the ruling provides international precedent to countries that wish to spread their repressive speech regimes to the rest of the world.[46] As Daphne Keller at Stanford University writes: "If Canada can enforce its laws to limit speech and information access in other countries . . . [c]an Russia use its anti-gay laws to make search results unavailable to Canadians?"[47] Global remedies awarded to repressive governments may also have the effect of suppressing criticism by defectors who now reside elsewhere and express their criticism online.[48] But repressive speech laws by authoritarian regimes are not the only concern, as even in democratic countries, speech norms such as the "right to be forgotten" are not standard everywhere.[49]

Second, the precedent set by *Equustek* may vest substantially greater power in the hands of internet intermediaries, with courts asserting jurisdiction over online activities and leaving intermediaries "as the arbiters of which laws to follow online."[50] The resulting legal uncertainty could have a chilling effect on international business investment. Alternatively, *Equustek* may encourage plaintiffs to engage in forum shopping for the country with the most favorable laws and seeking to have the remedy enforced across the global internet.[51]

While the *Equustek* decision has alarming implications for the free flow of ideas internationally, other courts have arrived at decisions that protect free expression. For example, the Stockholm Administrative Court in Sweden struck down a lower court injunction requiring global delisting of a newspaper article on Google, on the grounds that such an extraterritorial application of all

[44] Google Inc., v. Equustek Solutions, Inc., [2017] S.C.R. 824, 826 (Can.).
[45] *Id.* at 827-828.
[46] *See, e.g., Google Appeals French Data Protection Authority's Demand to Modify Search Results Worldwide*, *supra* note 74.
[47] Daphne Keller, *Ominous: Canadian Court Orders Google to Remove Search Results Globally*, CTR. FOR DEMOCRACY & TECH. (June 28, 2017, 11:31am), http://cyberlaw.stanford.edu/blog/2017/06/ominous-canadian-court-orders-google-remove-search-results-globally.
[48] *Id.* ("A critic of, say, the Vietnamese government may be safely ensconced in the US or Germany, far from the reach of Vietnamese state power. But her online speech is not.").
[49] Emma Llansó, *Global Application of French "Right to Be Forgotten" Law Would Pose Threat to Free Expression*, CTR. FOR DEMOCRACY & TECH. (Nov. 23, 2016), https://cdt.org/blog/global-application-of-french-right-to-be-forgotten-law-would-pose-threat-to-free-expression.
[50] Michael Geist, *Global Internet Takedown Orders Come to Canada: Supreme Court Upholds International Removal of Google Search Results*, MICHAELGEIST.CA (June 28, 2017), http://www.michaelgeist.ca/2017/06/global-internet-takedown-orders-come-canada-supreme-court-upholds-international-removal-google-search-results.
[51] *See* Comments to NTIA, *supra* note 13.

EU member states' laws to every search query was not a reasonable or foreseeable interpretation of data protection laws.[52]

RECOMMENDATION: Courts should never order a global removal of content from a platform, because doing so infringes upon the rights to information of citizens over whom they have no jurisdiction.

4. Regulatory Pressures Around Disinformation and "Fake News" Threaten Fundamental Rights.

Finally, we wish to highlight the issue of disinformation or so-called "fake news" as a particular challenge in global public policy discussions about the free flow of information online. While many governments and intermediaries are actively debating the issue and experimenting with potential solutions, uncertainty still abounds: about the definition of disinformation, evidence of its impact, and the effectiveness of potential solutions. Previous work has found a lack of consensus on the definition of "fake news," and a lack of credible evidence of the impact of disinformation across diverse domains.[53] Overwhelmingly, available studies are based on data from the US 2016 election.[54]

PEN America's comprehensive report on the topic, *Faking News: Fraudulent News and the Fight for Truth*, emphasizes that "[m]ore research, from a variety of perspectives, is required to help the public at large better understand new patterns of news consumption and how to prevent our fast-changing news ecosystem from buckling beneath the weight of polarization and mistrust."[55] And a 2017 Joint Statement by the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion, the Organization for Security and Cooperation in Europe, the Organization of American States, and the African Commission on Human Rights underscores the need for "creating a better understanding of the impact of disinformation and propaganda on democracy, freedom of expression, journalism and civic space, as well as appropriate responses."[56]

---

[52] Nedim Malovic*, Swedish Court Holds that Google Can Be Only Ordered to Undertake Limited Delisting in Right to Be Forgotten Cases*, THE IPKAT (May 5, 2018), https://ipkitten.blogspot.com/2018/05/swedish-court-holds-that-google-can-be.html.

[53] Jens-Henrik Jeppesen, *CDT's Response to EC 'Fake News' Consultation: How to Tackle the Issue and Protect Free Expression?*, CTR. FOR DEMOCRACY & TECH. (Jan. 30, 2018), https://cdt.org/blog/cdts-response-to-ec-fake-news-consultation-how-to-tackle-the-issue-and-protect-free-expression.

[54] *Id.*

[55] PEN AMERICA, FAKING NEWS: FRAUDULENT NEWS AND THE FIGHT FOR TRUTH 22 (2017), https://pen.org/faking-news [hereinafter FAKING NEWS].

[56] United Nations Special Rapporteur on Freedom of Opinion and Expression et al, Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda (Mar. 3, 2017), *https://www.osce.org/fom/302796* [hereinafter Joint Declaration on Freedom of Expression].

A danger of laws targeting disinformation is that weak rule-of-law states can capitalize on such international precedent to justify their own repressive policies.[57] Authoritarian regimes routinely suppress political dissent by leveraging uncertainty over what disinformation means, particularly by enacting laws criminalizing the dissemination of "false news"—but not defining "false news" in the statute. According to a 2018 Report of the UN Special Rapporteur: "Broadly worded restrictive laws on… 'false news' and 'propaganda' often serve as pretexts for demanding that companies suppress legitimate discourse."[58] The UN Special Rapporteur and others have condemned general prohibitions based on vague and ambiguous ideas like "false news" as being incompatible with international standards for restriction of free expression.[59]

China in particular has led the way in "enacting vaguely worded restrictions encouraging journalists to adhere to the official narrative or risk being branded false news and charged with a crime."[60] An amendment to Chinese criminal law threatens a prison sentence of up to 7 years for fabricating false information.[61] In Malaysia, a Danish citizen was sentenced to 1 week in prison and fined $2500 under the Anti-Fake News Act for posting a 2-minute video online criticizing police's response to the assassination of a member of Hamas in Kuala Lumpur.[62] At the end of 2016, at least 9 journalists were in jail worldwide for violating statutes on false news.[63]

Suppressing political dissent under the pretext of eradicating disinformation is particularly harmful during elections, when voicing political dissent may be most likely, and most effective. In 2018, for example, Egypt's General Prosecutor ordered state prosecutors to monitor media reports and take any actions against media outlets publishing "false news, [false] statements, and rumors" one month ahead of a presidential election in which President Abdel Fattah el-Sisi was running unopposed.[64] A February 2018 report found that at least 20 journalists were behind bars in Egypt since Dec. 1, 2017, over half of whom were detained for "spreading false news."[65]

Yet authoritarian governments are not the only ones who have proposed censorship rules under the broad goal of tackling disinformation. For example, a potential French law would

---

[57] *See* Comments to NTIA, *supra* note 13.
[58] Report of UN Special Rapporteur, *supra* note 19, at 6.
[59] Joint Declaration on Freedom of Expression, *supra* note 26.
[60] Courtney Radsch, *Deciding Who Decides Which News is Fake*, COMMITTEE TO PROTECT JOURNALISTS, (Mar. 14, 2017, 6:09 PM), https://cpj.org/blog/2017/03/deciding-who-decides-which-news-is-fake.php.
[61] Yaqiu Wang, *In China, Harsh Penalties for 'False News' Make It Harder for Reporters to Work*, COMMITTEE TO PROTECT JOURNALISTS, (Oct. 30, 2015, 5:29 PM), https://cpj.org/blog/2015/10/in-china-harsh-penalties-for-false-news-make-it-ha.php.
[62] *Malaysia Issues First 'Fake News' Conviction*, COMMITTEE TO PROTECT JOURNALISTS, (April 30, 2018, 12:28 PM), https://cpj.org/2018/04/malaysia-issues-first-fake-news-conviction.php.
[63] *Deciding Who Decides Which News is Fake*, *supra* note 31.
[64] Egypt's Top Prosecutor Orders Authorities to Monitor Media for "Fake News", COMMITTEE TO PROTECT JOURNALISTS, (Feb. 28, 2018, 4:58 PM), https://cpj.org/2018/02/egypts-top-prosecutor-orders-authorities-to-monito.php.
[65] *Id.*

have allowed the French government to censor fake news on the internet, particularly during election periods.[66] The EC has attempted to use concerns about disinformation to justify its (widely discredited) ancillary copyright proposal.[67] Documenting efforts by both authoritarian and democratic regimes across the globe to use "fake news" as a pretext to delegitimize the media, RPF has said: "Predators of press freedom have seized on the notion of 'fake news' to muzzle the media on the pretext of fighting false information."[68]

Even policies with non-pretextual motives for tackling disinformation may have unintended effects that outweigh any negative impacts of disinformation in the first instance[69]—though without careful research, this is impossible to know for sure. Disinformation laws can also put a thumb on the scale of entrenched news organizations, which are less likely to be characterized as disinformation than smaller, less mainstream, and less well-resourced outlets. The disappearance of legitimate but alternative press outlets could have a negative effect on the quality and scope of news, most likely at the expense of more marginalized groups or viewpoints.

RECOMMENDATION: NTIA should promote the important role of a robust, free press to a well functioning democracy. Policies that provide a pretext for undermining and delegitimizing journalism threaten the free flow of information. More research on the impact of disinformation on democracy, and on the effectiveness of potential solutions, should precede policymaking, and NTIA should encourage partner nations to carefully consider other policy responses such as transparency regarding the funding of political advertising.

II. Privacy & Cybersecurity Considerations in Emerging Technologies

1. NTIA Should Leverage Existing Expertise to Advance Privacy and Security Considerations in the Commercial Internet of Things Space.

The NTIA has solicited comment, first, on "what ways are cybersecurity threats harming international commerce" and second, on "[w]hat emerging technologies and trends should be the focus of international policy discussions." One obvious answer to both of these questions

[66] Glenn Greenwald, *First France, Now Brazil Unveils Plan to Empower the Government the Censor the Internet in the Name of Stopping "Fake News"*, THEINTERCEPT.COM (Jan. 10, 2018, 7:42AM), https://theintercept.com/2018/01/10/first-france-now-brazil-unveils-plans-to-empower-the-government-to-censure-the-internet-in-the-name-of-stopping-fake-news.

[67] Jens-Henrik Jeppesen & Lauren Blanco, *EC Initiative on Disinformation Must Not Curb Free Expression*, CTR. FOR DEMOCRACY & TECH. (April 27, 2018), https://cdt.org/blog/ec-initiative-on-disinformation-must-not-curb-free-expression.

[68] *Predators of Press Freedom Use Fake News as a Censorship Tool*, REPORTERS WITHOUT BORDERS (Mar. 17, 2017), https://rsf.org/en/news/predators-press-freedom-use-fake-news-censorship-tool.

[69] FAKING NEWS, *supra* note 25, at 4 ("The recognition of fraudulent news as a threat to free expression should not be employed as a justification for broad new government or corporate restrictions on speech, measures whose effects would be far more harmful to free speech.").

are data practices in the commercial Internet of Things (IoT) space. Both real and perceived privacy and security risks threaten public trust in and adoption of technologies that support the IoT, device connectivity, and "smart" products. As the NTIA has itself acknowledged, mistrust in company's online data stewardship inhibit online commerce, as well as other online activities,[70] and this is especially salient in IoT. Lack of privacy protections and adequate security "permeate the IoT," according to the Federal Trade Commission.[71]

Consumers and businesses agree that security in the IoT should be regulated. A 2017 survey of 1,050 IT and business decision makers, as well as 10,500 consumers, found that, "the vast majority of decision makers (96%) and consumer (90%) respondents state that there should be IoT security regulations."[72] Consumers are concerned not just with hackers or other bad actors, but also data leakage, uncontrolled sharing of information across multiple devices, unauthorized setting adjustments, and inadequate customer support.[73] Approximately 67% of U.S. respondents reported having "concerns that some digital technologies (e.g. self driving cars, smart homes and others) are unsafe,"[74] and these concerns are also reflected internationally amidst G20 nations. These problems are in large part caused by misaligned market incentives and one of the major suggested interventions, consumer education, has proved ineffective.

First, misaligned market incentives related to IoT or connected products generally encourage irresponsible data practices and technological development. CDT has previously written comments to the Consumer Product Safety Commission[75] on the safety implications of an under-regulated IoT environment and discussed how products liability doctrine could be useful to improve the wider IoT ecosystem.[76] At present, companies competing in the IoT space are racing to be first to market, as delays in delivering a product can be the difference between

[70] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[71] FTC STAFF REPORT, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD, FTC (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[72] *The State of IoT Security: Security Takes a Back Seat*, GERMALTO, (Oct. 31, 2017), https://www.gemalto.com/press/pages/gemalto-survey-confirms-that-consumers-lack-confidence-in-iot-device-security-.aspx.

[73] *Id.* at 13.

[74] CHRISTIAN THORUN ET. AL, INDICATORS OF CONSUMER PROTECTION AND EMPOWERMENT IN THE DIGITAL WORLD, INSTITUTE FOR CONSUMER POLICY 62 (Mar. 15, 2017), https://www.bmjv.de/G20/DE/ConsumerSummit/_documents/Downloads/Studie.pdf?__blob=publicationFile&v=1.

[75] Comments to CPSC on the Internet of Things and Consumer Product Hazards, CTR. FOR DEMOCRACY & TECH. (June 15, 2018), https://cdt.org/insight/comments-to-cpsc-on-the-internet-of-things-and-consumer-product-hazards/.

[76] Benjamin C. Dean, *Strict Products Liability and the Internet of Things*, CTR. FOR DEMOCRACY & TECH., https://cdt.org/files/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf.

market dominance or bankruptcy.[77] Since installing additional security measures, meaningful user controls, and following more rigorous software and hardware development processes can slow down development time, and thus time to market, companies are disincentivized to follow such processes.[78] Further, while upgradability and patchability are important benefits of the IoT, and should be built into devices and products, this functionality can actually incentivize developers to put out defective software under the auspices of being able to fix bugs down the road.[79] NTIA's multistakeholder process exploring IoT security upgradability and patching was useful.[80] While recognizing the benefits of being able to remotely patch/update a product, such functionality does not eliminate the need for strong security and privacy by design processes. Finally, firms lack a strong incentive to retroactively test products for security and software failures. If a firm discovers a flaw in a product's operational code, disclosing that flaw could lead to costly recalls and bad publicity.[81]

With respect to consumer education, consumers have limited insight or transparency into corporate data collection practices.[82] This is especially true for IoT devices, which make it difficult for users to make informed purchasing and data sharing decisions.[83] There is currently no widely-embraced security or safety certification program and associated labeling scheme for IoT devices.[84] Most efforts are still in their infancy,[85] and companies need further incentives to develop such programs. Additionally, software source code is protected by a litany of technical barriers and legal rules, and even if a consumer were able to access it, understanding the implications of code for data profiling, security, or safety would require the type of expert-level knowledge that the average consumer does not possess.[86] Furthermore, absent a security/safety certification or labeling scheme, manufacturers who use strong security practices are unable to differentiate themselves in the marketplace from others who use

---

[77] *Id.* at 3.

[78] Pfleeger S. L., Libicki M. and Webber M., "I'll buy that! Cybersecurity in the internet marketplace", IEEE Security & Privacy, Issue No. 03, Vol. 5 27 (May/June 2007).

[79] Benjamin C. Dean, *Strict Products Liability and the Internet of Things,* CTR. FOR DEMOCRACY & TECH. 3, https://cdt.org/files/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf.

[80] National Telecommunications and Information Administration, *Multistakeholder Process; Internet of Things Security Upgradability and Patching* (Nov. 7, 2017), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

[81] Arvinder Saini, *The Cost of Fixing Bugs Throughout the SDLC*, COMPUTER BUSINESS REVIEW (Mar. 1, 2017), https://www.cbronline.com/enterprise-it/software/cost-fixing-bugs-sdlc/.

[82] CHRISTIAN THORUN ET. AL, *supra* note 74.

[83] Benjamin C. Dean, *Strict Products Liability and the Internet of Things,* CTR. FOR DEMOCRACY & TECH. 3, https://cdt.org/files/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf.

[84] See *IoT Security for Policymakers,* INTERNET SOCIETY (Apr. 19, 2018), https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/.

[85] *See, e.g.*, *Principles for an Open Internet of Things Certification Mark*, OPEN INTERNET OF THINGS CERTIFICATION MARK (last updated June 13, 2018), https://iotmark.wordpress.com/principles/.

[86] Benjamin C. Dean, *Strict Products Liability and the Internet of Things,* CTR. FOR DEMOCRACY & TECH. 3, https://cdt.org/files/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf.

weaker standards.[87] Along these lines, CDT believes every IoT device should provide disclosures about its components. The NTIA has already announced that its next cybersecurity multistakeholder process will explore software component transparency.[88] CDT supports a requirement that all IoT devices contain a "Bill of Materials," which could contain a list of all component materials, parts, and software used in an IoT device.[89]

RECOMMENDATION: In response to the NTIA and its Internet Policy Task Force's green paper on advancing the IoT, CDT specifically recommended that the NTIA and the Department of Commerce further engage with stakeholders and pursue consensus-based global standards, starting from the premise that the data security and privacy challenges posed by the IoT are novel.[90] The Department is well positioned to highlight serious efforts to improve data governance, which includes addressing basic Fair Information Practice Principles and adopting privacy by design across the full lifecycle of IoT devices, products, and services.

IoT security deserves special consideration in light of global attacks such as the Mirai botnet, which was the result of systematic failures by governments, companies, and consumers to demand better security in our products.[91] CDT would encourage the NTIA to build on its existing expertise in the IoT ecosystem internationally. As CDT has noted in its comments to the NTIA on botnets and other automated threats,[92] effective cybersecurity policy will rest upon both public-private partnerships and meaningful participation by civil society. Global cybersecurity conversations must include digital liberties and consumer protection advocates, academics, and security researchers.

2. The United States Must Advance a Consistent Vision for Privacy and Data Protection Domestically and Abroad.

The NTIA has requested comment about the effectiveness of various international venues for engaging in conversations about emerging technologies. While CDT expresses no opinion on the merits of any particular international forum, global dialogues on privacy and data protection must inform ongoing U.S. privacy debates. At the 2017 convening in Hong Kong of the International Conference of Data Protection and Privacy Commissioners, it was apparent that the U.S. has ceded influence in global privacy debates to the European Union. Industries and

[87] *Id.* at 4.
[88] National Telecommunications and Information Administration, *NTIA Software Component Transparency* (June 5, 2018), https://www.ntia.doc.gov/SoftwareTransparency.
[89] Bill of Materials - BOM, INVESTOPEDIA, https://www.investopedia.com/terms/b/bill-of-materials.asp (Last visited July 10, 2018).
[90] Comments to the NTIA on Fostering the Advancement of the Internet of Things, CTR. FOR DEMOCRACY & TECH. (Mar. 10, 2017), https://cdt.org/insight/cdt-comments-to-the-ntia-on-fostering-the-advancement-of-the-internet-of-things/.
[91] Michelle De Mooy, *#IoTFail*, CTR. FOR DEMOCRACY & TECH., (Oct. 26, 2016), https://cdt.org/blog/iotfail/.
[92] CDT NTIA Botnet Comments, CTR. FOR DEMOCRACY & TECH., (Feb. 12, 2018), https://cdt.org/files/2018/02/CDT-NTIA-Botnet-Comments-Feb-2018.pdf.

commercial associations that once took their lead primarily from the privacy enforcement and education activities of the Federal Trade Commission are now operating in an environment dictated, on one hand, by the EU's General Data Protection Regulation and forthcoming ePrivacy Regulation[93] and, on the other, by efforts of individuals state such as Vermont's recently enacted data broker registration requirements[94] and California's more comprehensive Consumer Privacy Act of 2018.[95]

Regaining U.S. leadership on privacy and technology will require the Department of Commerce to advance its own vision of privacy that both acknowledges emerging global consensus on the importance of privacy-protective approaches to data processing and provides a flexible alternative.[96] In light of renewed interest since the revelations of unauthorized data use from the Facebook platform by Cambridge Analytica, Cameron Kerry, formerly of the Department of Commerce, and Daniel Weitzner, the former White House Deputy Chief Technology Officer for Internet Policy, have argued that U.S. policymakers should reconsider the aborted Consumer Privacy Bill of Rights as a potential "blueprint" for providing an "American answer" to more prescriptive privacy rules.[97] While there was much that was laudable in the Consumer Privacy Bill of Rights discussion draft, including its ambitious reliance on consumer expectations around the context in which information is processed,[98] the legislative proposal still relied on traditional notice-and-consent frameworks.

Moving forward, CDT believes any meaningful privacy framework will address three key themes: (1) **transparency**; (2) **control**; and (3) **autonomy**. International privacy norms must strive to grant reasonable degrees of information transparency, control, and autonomy to

---

[93] Trevor Butterworth, *Europe's tough new digital privacy law should be a model for US Policymakers,* VOX, (May 23, 2018), https://www.vox.com/the-big-idea/2018/3/26/17164022/gdpr-europe-privacy-rules-facebook-data-protection-eu-cambridge; Michael Birnbaum & Tony Romm, *Why Europe, not Congress, will rein in big tech,* WASHINGTON POST, (Apr. 15, 2018), https://www.washingtonpost.com/world/europe/why-europe-not-congress-will-rein-in-big-tech/2018/04/14/a39c8cd8-2e33-11e8-8dc9-3b51e028b845_story.html?noredirect=on&utm_term=.7e72adf73b0c; Mark Scott & Laurens Cerulus, *Europe's new data protection rules export privacy standards worldwide,* POLITICO (Jan. 13, 2018), https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/.

[94] Vermont H.764 (2018).

[95] California Consumer Privacy Act of 2018, AB 375.

[96] Cameron F. Kerry, *Why protecting privacy is a losing game today - and how to change the game,* BOOKINGS, (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ ("We need an American answer—a more common law approach adaptable to changes in technology—to enable data-driven knowledge and innovation while laying out guardrails to protect privacy.").

[97] *Id*. *See also*, Daniel J. Weitzner, *How Cambridge Analytica, Facebook and Other Privacy Abuses Could Have Been Prevented,* LAWFARE, (Apr. 4, 2018), https://www.lawfareblog.com/how-cambridge-analytica-facebook-and-other-privacy-abuses-could-have-been-prevented.

[98] Analysis of the Consumer Privacy Bill of Rights Act, CTR. FOR DEMOCRACY & TECH, (Mar. 2, 2015), https://cdt.org/insight/analysis-of-the-consumer-privacy-bill-of-rights-act/.

individuals online and off.[99] Transparency into what data is collected – why, how, and by whom – is an important first step, but an accurate understanding of how that data could be shared with other parties or used to make automated decisions is also essential. Individual rights to access information and correct, delete, or "port" it from a particular platform, service, or company is also an important element of control.[100]

Such rights are meaningless, however, if individuals are unaware of their individual rights or the means of accessing them. While expanded individual rights to information could serve to counterbalance the risk of privacy violations, fundamental information asymmetries limit an individual's ability to make informed decisions about privacy and security and the processing of their information.[101] This asymmetry is heavily weighted toward corporate interests, and individual users are left to navigate opaque data ecosystems that are beyond their comprehension.[102] Ordinary, and often even sophisticated, internet users cannot meaningfully understand or consent to such complex and obscure data practices.[103]

Further, a privacy framework that stresses only formalistic transparency and control requirements is insufficient to facilitate personal autonomy, or informational self-determination in the digital age.[104] Autonomy is an important cornerstone of any free and democratic society, and necessary for freedom of thought, the marketplace of ideas, and the ability to engage in meaningful and critical discourse. On a more fundamental level, when individuals are stripped of adequate autonomy, their decisions cease to reflect a free expression of their own will. Privacy protections explicitly facilitate important values like freedom of thought, belief, and association, as well as intimate decisions that should be shielded from public view.[105]

RECOMMENDATION: New policy approaches, backed by rigorous regulatory enforcement, is necessary to rebalance these informational asymmetries. For the United States, we reiterate

---

[99] Nuala O'Connor, *The Big Questions About Privacy That Need Answer*, CTR. FOR DEMOCRACY & TECH. (Apr. 9, 2018), https://cdt.org/blog/the-big-questions-about-privacy-that-need-answers/.
[100] *Id.*
[101] CDT FTC Informational Injury Comments, Ctr. for Democracy & Tech., (Oct. 27, 2017), https://cdt.org/files/2017/10/2017-1027-CDT-FTC-Informational-Injury-Comments.pdf.
[102] Nuala O'Connor, *The Big Questions About Privacy That Need Answer*, CTR. FOR DEMOCRACY & TECH. (Apr. 9, 2018), https://cdt.org/blog/the-big-questions-about-privacy-that-need-answers/; *See also* Off. of the Attn. Gen. Dept. of Fin. Reg., Report to the General Assembly of the Data Broker Working Group issued pursuant to Act 66 of 2017 (Dec. 15, 2017), http://ago.vermont.gov/wp-content/uploads/2018/02/2017-12-15-Data-Broker-Working-Group-Report.pdf.
[103] Zeynep Tufekci, *The Latest Data Privacy Debacle*, N.Y. TIMES, (Jan. 30, 2018), https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html.
[104] "Informational self-determination" emerges from a German Federal Constitutional Court decision. Bundesverfassungsgericht [BVerfGE] [Federal Constitutional Court] 1 BvR 209/83, Dec. 15, 1983. It is far broader than traditional privacy frameworks that emphasized individuals' right to be left alone.
[105] Julie Cohen, *Privacy, Autonomy, and Information 4, Configuring the Networked Self*, JULIECOHEN.COM (2012) www.juliecohen.com/attachments/File/CohenCNSCh5.pdf.

our call for comprehensive privacy legislation that is consistent with emerging global privacy standards and encourage NTIA to embrace the need for a legislative solution. Internationally, the Department of Commerce should encourage data protection authorities and regulators to use their enforcement powers strategically and focus on the most problematic data practices to address this vast power differential.

The NTIA will also need to engage with companies and other civil society stakeholders. Companies must also do more to counter unintentional biases within their systems, and to rapidly adjust these systems and the values embedded in them when they lead to unjust outcomes.[106] CDT is a regular participant in the Partnership on AI, which is a global collaboration between industry, civil society, and researchers to to study and formulate best practices on machine learning, automated decision-making, and artificial intelligence.[107] The Department of Commerce must keep itself informed of the latest developments from such non-governmental multi-stakeholder groups and may wish to weigh in as appropriate.

3. Encryption Is Vital to the Continuing Use of and Trust in the Internet and the Growth of the U.S. Economy.

Everyday people around the world use the internet to share ideas, conduct financial transactions, and keep in touch with loved ones and colleagues. They send and store intimate conversations, personal medical data, and business communications online. In order for the internet to continue to grow, thrive, and further be integrated into the U.S. economy, people must trust that their personal information will be secure and their privacy protected. Absent the use of encryption, all these communications and records are fundamentally insecure. Anyone with access to the servers that store our data or the networks that transmit them would be able to intercept any communication, or alter and delete them.

Encryption is vital to addressing this fundamental vulnerability. Properly deployed, encryption ensures that journalists, dissidents, and neighbors can safely use the internet to freely express their ideas and to report on governmental abuses. Indeed, this was observed by David Kaye, UN Special Rapporteur on the freedom of opinion and expression, "Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks."[108] Encryption promises, too, to protect all of our digital assets from the increasingly frequent and costly cyber

[106] See Natasha Duarte, *Digital Decisions Tool*, CTR. FOR DEMOCRACY & TECH. (Aug. 8, 2017), https://cdt.org/blog/digital-decisions-tool/; *Digital Decisions*, CTR. FOR DEMOCRACY & TECH., https://cdt.org/issue/privacy-data/digital-decisions/ (last visited July 16, 2018).
[107] *About Us*, PARTNERSHIP ON AI (last visited on July 11, 2018), https://www.partnershiponai.org/about/.
[108] Report of the Special Rapporteur on the on the promotion and protection of the right to freedom of opinion and expression, *Report on encryption, anonymity, and the human rights framework,* Human Rights Council, U.N. Doc. A/HRC/29/32 (May 22, 2015) (by David Kaye) 7, https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx.

attacks that have exposed so much sensitive information to malicious hackers or oppressive regimes.[109]

The health of the U.S. economy depends on encryption. The U.S. has a strong interest in promoting the continued growth of internet based services as the world's current commercial leader in such enterprises. The internet sector was responsible for an estimated $966.2 billion, or six percent, of real GDP in 2014.[110] However, the cost associated with and risk of data breaches continue to grow.[111] Ensuring that encryption is widely adopted, and not weakened is vital to ensuring that people continue to trust and use the internet, and consequently the growth of the U.S. economy.

Many services and products today have built in encryption that keep communications content secure. Consumers are most familiar with the cryptography that keeps internet connections secure: the HTTPS protocol. HTTPS enables consumers to complete secure online transactions like paying credit cards bills, applying for public benefits and uploading photos to social media platforms.[112] Furthermore, Apple and Google have made encryption default features of their products[113] and encrypted messaging apps like Signal and Telegram are proliferating.[114] All of

[109] *See, e.g.*, *Security breach at MyHeritage website leaks details of over 92 million users,* REUTERS (June 5, 2018), https://www.reuters.com/article/us-myheritage-privacy/security-breach-at-myheritage-website-leaks-details-of-over-92-million-users-idUSKCN1J1308; Lisa Maria Segarra, *Under Armour Data Breach Exposes 150 Million MyFitnessPal Accounts*, TIME (Mar. 30, 2018) http://time.com/5222015/under-armour-myfitnesspal-data-breach/; Todd Shields & Eric Newcomer, *Uber's 2016 Breach Affected More Than 20 Million U.S. Users*, BLOOMBERG (Apr. 12, 2018), https://www.bloomberg.com/news/articles/2018-04-12/uber-breach-exposed-names-emails-of-more-than-20-million-users; Selena Larson, *Every single Yahoo account was hacked-3 billion in all Yahoo*, CNN (Oct. 4, 2017), https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html; John McCrank & Jim Finkle, *Equifax breach could be most costly in corporate history*, REUTERS (Mar. 2, 2018), https://www.reuters.com/article/us-equifax-cyber/equifax-breach-could-be-most-costly-in-corporate-history-idUSKCN1GE257; Brendan Koerner, *Inside The Cyberattack That Shocked The US Government*, WIRED (Oct. 23, 2016), https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

[110] STEPHEN E. SIWEK, MEASURING THE U.S. INTERNET SECTOR, INTERNET ASSOCIATION 5 (2015), https://cdn1.internetassociation.org/wp-content/uploads/2015/12/Internet-Association-Measuring-the-US-Internet-Sector-12-10-15.pdf.

[111] A 2018 report sponsored by IBM Security found that the average cost of a data breach globally is $3.86 million, a 6.4 percent increase from the 2017 report. IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses, IBM NEWS ROOM (July 11, 2018), http://newsroom.ibm.com/2018-07-11-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses#assets_117:19380. Furthermore, the White estimated that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016. COUNCIL OF ECONOMIC ADVISORS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY, WHITE HOUSE, 1 (2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[112] BEYOND SECRETS: THE CONSUMER STAKE IN THE ENCRYPTION DEBATE, CONSUMERS UNION, 9 (2017), https://consumersunion.org/wp-content/uploads/2017/12/Beyond-Secrets-12.21.17-FINAL.pdf.

[113] *Privacy*, APPLE INC, (2018), https://www.apple.com/privacy/approach-to-privacy/; *Products & Capabilities*, GOOGLE, (last visited July 17, 2018), https://cloud.google.com/security/products/.

these tools enable the estimated 299 million Americans who use the internet to do so with confidence in the security of their transactions.[115]

An obstacle to the adoption of strong encryption practices continues to be law enforcement. In the U.S. context, the Federal Bureau of Investigation ('FBI') advocates for the creation of "back door" access into encrypted products like smartphones. This is necessary to combat what they term as the "going dark" problem, or the inability of law enforcement to access the content of communications protected by encryption. Notably, in the wake of the San Bernardino shooting, the FBI called for companies to build security flaws into their encrypted products so that the government could break through and wiretap consumers or seize data stored on their devices.[116] The FBI sought to force Apple, Inc. to produce an insecure version of its mobile operating system in order to gain access to the terrorist's device. Apple refused and this conflict spurred a court battle that was ultimately abandoned once the FBI was able to gain access into the device without Apple's assistance. A recent IG report reviewing the investigation found that a key entity within the FBI was not even asked for assistance to gain access to the encrypted iPhone until a few days before the DOJ sued Apple to compel it to build a backdoor into the iPhone.[117] Furthermore, another recent report also confirmed that the FBI inflated the number of locked devices it cannot open.[118] Both of these revelations cast doubt on the FBI's argument that they are indeed going dark.

Need aside, calls for backdoor access or key escrow systems are not viable solutions. It is abundantly clear that such tactics would undermine security for all while being trivially easy for law enforcement's adversaries to circumvent.[119] Security experts have concluded so for years.[120] In other words, making devices inherently vulnerability to one actor (law enforcement) would also make devices vulnerable to bad actors like hackers, and foreign adversaries.

---

[114] See Ioana Rijnetu, *The Best Encrypted Messaging Apps You Should Use Today [Updated]*, HEIMDAL SECURITY, (June 21, 2018), https://heimdalsecurity.com/blog/the-best-encrypted-messaging-apps/.

[115] STEPHEN E. SIWEK, MEASURING THE U.S. INTERNET SECTOR, INTERNET ASSOCIATION 4 (2015), https://cdn1.internetassociation.org/wp-content/uploads/2015/12/Internet-Association-Measuring-the-US-Internet-Sector-12-10-15.pdf.

[116] Greg Nojeim, *Inspector General: FBI Chomping at the Bit for Backdoors to Encryption*, CTR. FOR DEMOCRACY & TECH, (Apr. 4, 2018), https://cdt.org/blog/inspector-general-fbi-chomping-at-the-bit-for-backdoors-to-encryption/.

[117] *Id*.

[118] Press Release, FBI's "Going Dark" Claims Now Even More Dubious, CTR. FOR DEMOCRACY & TECH, (May 22, 2018), https://cdt.org/press/fbis-going-dark-claims-now-even-more-dubious/.

[119] *See, e.g.*, Joseph Lorenzo Hall, *Strong Encryption Has A Posse*, CTR. FOR DEMOCRACY & TECH, (May 20, 2015), https://cdt.org/blog/strong-encryption-has-a-posse/; Hal Abelson e. al, *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*, 1997 (Columbia University Academic Commons) *available at* https://www.cdt.org/files/pdfs/paper-key-escrow.pdf.

[120] Harold Abelson, et al., Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, July 7, 2015, *available at* https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf.

Acquiescing to these demands for access would be bad for commercial entities in the U.S.. Consumers outside of the US may be less inclined to purchase American tech products that facilitate government surveillance. Consider, for example, the difficulty US companies would have selling smartphones or network servers in the EU that are built to enable easy access for the NSA. Furthermore, as a technical matter, it is difficult and expensive to both build a backdoor security vulnerability and then defend that vulnerability against unauthorized use. This burden would be heaviest on small businesses and innovators of new communications services. Consequently such actors may be disincentivized to encrypt their products and services, which would reduce the overall security of users.

These policy debates are being held around the world. Many countries, like Iran, outright ban encrypted technologies.[121] Turkey, during the failed coup in 2016, arrested individuals who downloaded an encrypted messaging app.[122] Russia recently demanded access to Telegram communications and when denied banned the service.[123] Furthermore like the U.S. government, foreign governments are also trying weaken encryption and gain backdoor access to devices. In 2016 the United Kingdom passed the Investigatory Powers Act, which may provide the government the authority to weaken encryption.[124] Australia may be following in the UK's footsteps.[125]

RECOMMENDATION: The NTIA itself recognized that their "policy work is grounded in the belief that cybersecurity risks should be viewed not exclusively as a national security threat, but as a threat to economic growth and innovation."[126] To this end, as an arm of the Department of Commerce it is vital that NTIA encourage strong encryption adoption by companies, and work with the international community to set norms that permit encryption to be adopted and preserved.

---

[121] See Computer Crimes Act, Jan. 23, 2010, https://www.unodc.org/res/cld/document/computer-crimes-act_html/Computer_Crimes_Act.pdf.

[122] Owen Bowcott, *Turks detained for using encrypted app 'had human rights breached'*, THE GUARDIAN, (Sept. 11, 2017), https://www.theguardian.com/world/2017/sep/11/turks-detained-encrypted-bylock-messaging-app-human-rights-breached.

[123] Jack Stubbs & Andrey Ostroukh, *Russia to ban Telegram messenger over encryption dispute*, REUTERS, (April 13, 2018), https://www.reuters.com/article/us-russia-telegram-block/russian-court-bans-access-to-telegram-messenger-idUSKBN1HK10B.

[124] Greg Nojeim & Christine Galvagna, *UK Investigatory Powers Bill Imperils Public Safety by Undermining Data Sharing with the US*, CTR. FOR DEMOCRACY & TECH, (Sept. 6, 2016), ttps://cdt.org/blog/uk-investigatory-powers-bill-imperils-public-safety-by-undermining-data-sharing-with-the-us/.

[125] Amy Remeikis, *Australian bill to create back door into encrypted apps in 'advanced stages',* THE GUARDIAN, (Apr. 12, 2018), https://www.theguardian.com/technology/2018/apr/13/australian-bill-to-create-back-door-into-encrypted-apps-in-advanced-stages.

[126] See National Telecommunications and Information Administration, U.S. Department of Commerce, International Internet Policy Priorities (Federal Register Number Docket No. 2018-12075), (June 5, 2018) https://www.federalregister.gov/documents/2018/06/05/2018-12075/international-internet-policy-priorities.

4. Governments Must be Encouraged to Develop A Transparent and Formal Vulnerability Disclosure Process.

As more formerly unconnected devices are connected to the internet, and more of people's lives are driven by data, computation, and networking, software vulnerabilities carry increasing risk and cost to people, businesses and the economy. Compromised systems and devices have been used to launch attacks all over the world at great cost to people and companies. As the NTIA itself observed "[f]inding these vulnerabilities and informing affected parties is essential to protect our economy and citizens."[127]

Government actors are faced with unique and at times competing obligations. They are tasked with protecting a nation, which includes gathering intelligence and strengthening military operations. As the internet has been further integrated into our economy, and day to day lives, opportunities for new methods of attacking adversaries and collecting intel have emerged through the use of "zero-day exploits." A government may identity such an exploit and desire the opportunity to deploy it covertly in furtherance of its national security responsibilities. At the same time, the longer a vulnerability is not disclosed the greater the risk that a bad actor, hackers or a foreign adversary, identify the very same vulnerability and exploit it themselves. As massive data breaches occur, the cost associated with these exploits have become clearer. Indeed, the NSA was accused of failing to release a vulnerability prior to a major hack.[128] Governments need to develop a strategy to determine how to balance the equities in these situations, something the US has taken the lead on.[129]

In 2017 the White House released its Vulnerabilities Equities Process ('VEP'), a White House-convened process for deciding whether the government will keep vulnerabilities for its own use, or notify companies of their existence so they can be patched.[130] The release of this charter was a positive step toward increasing transparency about this controversial process. The charter makes clear that government-discovered vulnerabilities should be disclosed unless there is a demonstrable law enforcement or intelligence reason to retain them. The list of considerations to guide any single determination is a clear recognition of how high the stakes

---

[127] NTIA AWARENESS AND ADOPTION GROUP, VULNERABILITY DISCLOSURE ATTITUDES AND ACTIONS, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, 3 (2016), https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf.

[128] Kim Zetter, *Has The NSA Been Using The Heartbleed Bug as an Internet Peephole?,* WIRED (April 10, 2014), https://www.wired.com/2014/04/nsa-heartbleed/.

[129] Michelle Richardson, *Here's What The White House Needs to Disclose About Its Vulnerabilities Process This Month*, CTR. FOR DEMOCRACY & TECH, (Nov. 1, 2017), https://cdt.org/blog/heres-what-the-white-house-needs-to-disclose-about-its-vulnerabilities-process-this-month/.

[130] *Vulnerabilities Equities Policy and Process for the United States Government*, WHITE HOUSE (Nov. 15, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

are. And finally, the charter is an example of how a country can be transparent and thoughtful about its responsibility to report discovered vulnerabilities.

RECOMMENDATION: The U.S. is but one government in a borderless internet ecosystem, and vulnerabilities can be discovered and operationalized by any government; indeed, more governments are incorporating cyber into their military capabilities.[131] To encourage thoughtful balancing of equities by foreign governments, NTIA should work with its foreign counterparts to create transparent, thoughtful vulnerabilities equities processes of their own.

5. **Cross-Border Data Demand Agreements Must Include Human Rights Safeguards to Preserve U.S. Companies' Competitive Edge.**

Law enforcement officials in the United States and abroad increasingly seek access to electronic communications, such as emails and social media posts, that are stored on servers and in data centers in foreign countries. One reality of the internet as designed today is that a company can store data in servers far removed from the location of their customers. As a result, evidence to solve a crime committed in one country may exist in the territory of another. The primary method of resolving this problem has been through the development of Mutual Legal Assistance Treaties ('MLAT'), bilateral agreements that detail an agreed upon process by which law enforcement may request information stored in the other's territory. For example, if an investigating official in France needs communications content of a Gmail user in France to investigate a crime, she does not make the request directly to Google, but rather approaches a central authority in France which makes a request for mutual legal assistance of the US Department of Justice (DOJ), which can provide that assistance by applying for a warrant to serve on Google to compel disclosure of this information. It is widely perceived that MLAT processes are too slow for law enforcement investigations in the digital era and that they are not up to the task of dealing with the volume of cross-border demands for data that law enforcement agencies need to make.

Partially in response to the perception that MLATs needed to change Congress passed the "Clarifying Lawful Overseas Use of Data Act" ('CLOUD Act') as part of an omnibus spending bill earlier this year. The legislation authorizes the Department of Justice to enter into agreements with foreign governments allowing those governments to make direct demands to U.S. technology companies for content and metadata under their own laws instead of using existing mutual legal assistance treaties. It also authorizes the U.S. Department of Justice to make demands for data stored abroad by U.S. communications service providers.

[131] See Joint Statement for the Record to the Senate Armed Services Foreign Cyber Threats to the United States, The Honorable James R. Clapper, The Honorable Marcel Lettre & Michael S. Rogers, (Jan. 5, 2017), https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.

CDT opposed the passage of the CLOUD Act because the legislation does not adequately ensure human rights protection in these agreements, and we have raised serious concerns about its practical implementation.[132] In deciding whether to certify a country for a bilateral agreement the law requires that the Attorney General (AG) determine that "the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties." The factors the AG must consider in making this determination are stated broadly, and they include whether the country prohibits torture, guarantees fair trials and prohibits arbitrary arrests, protects against wrongful interference with privacy, and protects free expression. However, given the political nature of determining a country is not human rights compliant, the AG may well certify a country in spite of such failings. Furthermore, the CLOUD Act does not clearly mandate that the other country's legal system requires judicial authorization for data requests. It also permits certifications to last for five years, a timeframe during which it is foreseeable that a country's adherence to human rights principles may change. The Cloud Act raises many doubts that even the meager protections it requires will prevail, making it important that the NTIA assume a monitoring role.

By creating authority for the U.S. Department of Justice to issue legal process with extraterritorial effect, the CLOUD Act also opens up questions about the legal process required to obtain the contents of communications of foreigners abroad. Precedents based on the Fourth Amendment to the U.S. Constitution, such as *U.S. v. Warshak*,[133] which requires the use of warrants to obtain communications content, might not be considered to apply when the U.S. is seeking the content of foreigners outside the U.S.. In the absence of legislation requiring warrants for content, NTIA should ensure ensure that the current U.S. policy of requiring DOJ to get a warrant to obtain communications content stays in tact, and applies on a non-discriminatory basis to protect the content of people no matter their nationality. Any backpedaling on this protection would call into question the ability of U.S. providers to adequately protect content of foreign companies and persons against unfounded demands for it from the U.S. government. It would put U.S. providers at a competitive disadvantage.

RECOMMENDATION: The NTIA should recognize that the Cloud Act will have an impact on cross-border data demands. While it is not one of the agencies charged with executing the CLOUD Act, NTIA has expertise that could provide value to the implementation of the CLOUD Act, and should make itself available to the agencies tasked with implementing the legislation. In particular, the NTIA should point out the negative competitive effect on U.S. companies that would result from any backpedaling on the warrant-for-content policy now in place at the Department of Justice.

***

[132] For additional information on the outstanding issues that require resolution, please see: Greg Nojeim, *Cloud Act Implementation Issues*, LAWFARE (July 10, 2018), https://www.lawfareblog.com/cloud-act-implementation-issues.
[133] 631 F.3d 266 (6th Cir. Dec. 2010).

We greatly appreciate the opportunity to submit these comments to the NTIA in its inquiry on international internet policy priorities. CDT believes in the power of the internet. Whether it's facilitating entrepreneurial endeavors, providing access to new markets and opportunities, or creating a platform for free speech, the internet empowers, emboldens and equalizes people around the world. We hope the NTIA's work can help the internet remain open, innovative and free.

Sincerely,

Emma Llansó
Director, Free Expression Project

Joseph Jerome
Policy Counsel, Privacy and Data

Michelle Richardson
Deputy Director, Freedom, Security and Technology Project

Greg Nojeim
Director, Freedom, Security and Technology Project