CENTER FOR DEMOCRACY & TECHNOLOGY

Analysis, Assessments, and Audits

From CDT's *Making Transparency Meaningful: A Framework for Policymakers*

A key mechanism of tech company accountability is analysis of the company's business practices for their effects on individuals or their compliance with specific criteria. This analysis can take a variety of forms. For example, risk assessments are forward-looking, focused on the risks that a company's products or services pose and how the company can mitigate those risks. Audits, in contrast, are generally backwards-looking and focused on evaluating whether the company has met an objective set of standards or criteria. Both assessments and audits may be conducted internally or by independent third parties. A primary goal of an audit is to provide the auditor's assurance that a company is meeting a particular standard. This does not always involve furnishing a detailed public report; in many cases, the auditor's opinion that the organization is in compliance with the audit criteria provides sufficient assurance. However, if a public report is published following an assessment or audit, it can offer some transparency about how a technology company operates and its impacts on the speech and privacy rights of users and communities. Third-party assessments or audits, in particular, can be important mechanisms for holding companies accountable to their commitments and stated policies.

////

Current Assessments and Audits

Some technology companies engage in risk assessments that they make available to the public. For example, Human Rights Impact Assessments (HRIAs) are an increasingly popular, though still rare, form of risk assessment focused on the impact of a technology company's practices and services on human rights.[1] The UN Guiding Principles on Business and Human Rights provide a set of guidelines for States and companies to prevent and address human rights abuses committed in business operations, which

1 Other stakeholders in the technology field also publish HRIAs; for example, the Global Internet Forum to Counter Terrorism, an NGO founded by technology companies to increase collaboration on online counterrorism efforts, recently published its first HRIA, BSR, *Human Rights Assessment: Global Internet Forum to Counter Terrorism*, BSR.org (2021), following advocacy from a coalition of human rights organizations. *See* Ctr. Democracy & Tech., *Human Rights NGOs in Coalition Letter to GIFCT* (July 30, 2020).

includes the expectation that companies will carry out human rights due diligence.[2] HRIAs are "a systematic approach to due diligence" through which a company examines "how its products, services, and business practices affect the freedom of expression and privacy of its users."[3] Companies may publish an annual human rights report[4] or discrete HRIAs on particular topics, such as a new or existing product or service[5] or their operation in particular countries.[6] The proposed Article 26 of the Digital Services Act in Europe would require certain ICT companies to engage in yearly risk assessments that consider certain specified risks, including their services' impact on particular human rights.[7]

Third parties also conduct analyses or assessments, either independently or in cooperation with the technology company, of whether company practice meets a set of pre-defined standards or criteria for responsible business practices, and publish these analyses or assessments publicly. Prominent examples include:

- Company Assessments by the Global Network Initiative (GNI), through which GNI independently assesses member companies on their progress in implementing the GNI Global Principles on Freedom of Expression and Privacy[8] with improvement over time, using a confidential review of companies' "systems, policies, and procedures" and responses to case studies.[9] GNI publishes a summary of each cycle's assessment process but the detailed reports remain confidential to the GNI Board;[10]

- The Ranking Digital Rights Corporate Accountability Index, an annual "evaluat[ion of] 26 of the world's most powerful digital platforms and telecommunications companies on their disclosed policies and practices

2 UN Working Grp. on Bus. & Human Rights, *The UN Guiding Principles On Business And Human Rights: An Introduction*, Office of the High Commissioner for Human Rights (last visited Nov. 30, 2021); BSR, *Conducting an Effective Human Rights Impact Assessment*, BSR.org (Mar. 2013). The UN B-Tech Project continues this important work, providing additional guidance on conducting human rights due diligence in the tech sector. *B-Tech foundational paper | Identifying human rights risks related to end-use*, Bus. & Human Rights Resource Ctr. (Dec. 14, 2020).

3 *2020 Indicators*, Ranking Digital Rights (last visited Nov. 30, 2021).

4 *See, e.g.*, *Corporate Social Responsibility*, Microsoft (last visited Nov. 30, 2021) (linking to the Microsoft Annual Human Rights Report).

5 BSR, *Google Celebrity Recognition API Human Rights Assessment | Executive Summary*, BSR.org (Oct. 2019).

6 *See, e.g.*, BSR, *Human Rights Assessment: Facebook in Myanmar*, Facebook (Oct. 2018); Chloe Poynton, *Our Assessment of Facebook's Human Rights Impacts in Sri Lanka & Indonesia*, Article One (May 12, 2020). As in these examples, companies often work with third-parties to conduct HRIAs.

7 Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, at Art. 26, COM (2020) 825 final (Dec. 15, 2020) [hereinafter "Digital Services Act"].

8 *The GNI Principles*, Global Network Initiative (last visited Nov. 30, 2021).

9 *Company Assessments*, Global Network Initiative (last visited Nov. 30, 2021).

10 *The GNI Principles at Work: Public Report on the Third Cycle of Independent Assessments of GNI Company Members 2018/2019*, Global Network Initiative (last visited Nov. 30, 2021).

affecting people's rights to freedom of expression and privacy," based on dozens of indicators in three main categories: governance, freedom of expression and information, and privacy;[11] and

- The Facebook Oversight Board, an independent body founded by Facebook to review Facebook and Instagram's content moderation decisions and issue policy advisory opinions on the company's content policies, which operates in a quasi-judicial style by reviewing individual cases against Facebook's values and community guidelines as well as international human rights standards, and publishing its decisions.[12]

Finally, independent third parties may also conduct and publish audits of technology companies, which are the systematic and independent collection and evaluation of objective evidence to determine whether specified audit criteria are fulfilled.[13] Technology companies may be covered by a variety of formal auditing requirements, including financial audits, privacy audits, and other evaluations of their compliance with particular regulations; often, these types of audits are not made available to the public and therefore do not serve a material transparency purpose.[14] In the past few years, however, several companies have also submitted to voluntary audits of their company practices based on concerns over systemic bias in the company's products, internal policies, or organizational structure.[15] These audits are often commissioned by a company, but they are conducted by independent third parties, such as a law firm or professional auditing firm. For example, in 2020, civil rights and civil liberties leader Laura W. Murphy and the law firm Relman Colfax PLLC published a final report on their Facebook Civil Rights Audit, which Facebook commissioned at the request of the civil rights community.[16] The field of civil rights auditing in the U.S. is nascent and the standards and practices for such audits are still in development.[17] The proposed Article 28 of the EU Digital Services Act would require certain very large online services to undergo formal yearly audits evaluating their compliance with various requirements in

11 *The 2020 RDR Index*, Ranking Digital Rights (last visited Nov. 30, 2021).

12 *Governance*, Oversight Bd. (last visited Nov. 30, 2021).

13 *See ISO 19011:2018(en) Guidelines for auditing management systems* at 3.1, International Organization for Standardization (last visited Nov. 30, 2021) (defining "audit").

14 *See, e.g.*, Michelle De Mooy, *How to Strengthen the FTC Privacy & Security Consent Decrees*, Ctr. for Democracy & Tech. (Apr. 12, 2018) (explaining that FTC privacy assessments of technology companies are not readily publicly available); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 at Art. 35 (requiring Data Protection Impact Assessments).

15 Laura W. Murphy, *Airbnb's Work to Fight Discrimination and Build Inclusion*, Airbnb (Sept. 8, 2016); *Three Year Review — Airbnb's Work to Fight Discrimination and Build Inclusion*, Airbnb (Sept. 10, 2019).

16 *Facebook's Civil Rights Audit – Final Report*, Facebook (July 8, 2020). Several chapters of the report addressed free expression issues such as content moderation and one chapter explicitly addressed privacy.

17 Laura W. Murphy, *The Rationale for and Key Elements of a Business Civil Rights Audit*, Leadership Conference on Civil & Human Rights (2021).

the Act; Article 33 would require companies to publish these audit reports along with a report on their implementation of any recommendations in the audit report.[18]

////

Improving Analysis, Assessments, and Audits: Considering Tradeoffs

Who should conduct analysis, assessments, and audits, and what criteria should independent assessors and auditors be required to meet?

Self-assessments allow companies to draw on their expertise and familiarity with their services to provide an evaluation that may be more holistic than that by an outside assessor or auditor. Self-assessments may also be significantly less expensive and more achievable for smaller and newer companies. However, self-assessments raise concerns about bias, *i.e.*, whether a company is objectively and impartially evaluating the effects of services on individuals' speech and privacy or the potentially discriminatory impact of their systems, and whether they have the cultural competency or other expertise to do so.

Third-party analysis, assessments, and audits may lessen concerns about bias, but only if the auditors and assessors are truly independent and are perceived as independent; assessors and auditors also need to have the requisite cultural competence and expertise. Accordingly, any voluntary or mandatory regime of third-party assessments and audits should establish requirements of independence and competency. Requirements for independence could include financial independence from the company being assessed or audited and elimination of other potential conflicts of interest, such as familial or business relationships between the assessor or auditor and the company. Important qualifications of assessors or auditors to consider are whether they have sufficient professional experience with and knowledge of technology companies and human rights, including free expression and privacy, as well as familiarity with the specific cultural context(s) in which the technologies are being used.

If assessments or audits are legally required, it may be necessary to establish a formal accreditation mechanism for assessors or auditors. Other forms of auditing may be helpful references for requirements or accreditation processes for assessors and auditors, such as international standards governing Environmental, Social, or Governance audits[19] or the International Organization for Standardization's

18 Digital Services Act, *supra* n.7 at Art. 28.

19 *See* ESG reporting and attestation: A roadmap for audit practitioners, Association of International Certified Professional Accountants & Center for Audit Quality (Feb. 2021).

requirements for accreditation bodies accrediting conformity assessment bodies.[20] These models may prove especially useful as the nascent assessments and audits of technology companies with respect to their business practices concerning speech, privacy from government surveillance, access to information, and other human rights are further developed.

What services should be assessed or audited and what are the appropriate assessment or audit procedures and criteria?

Different technology companies offer different services, and assessment and audit methods that may be appropriate for some services may not work for others. For example, an assessment or audit to evaluate the risks to speech and privacy caused by a social networking platform's use of algorithms in content moderation will need to examine different data from an assessment or audit of the risks to speech and privacy posed by a search engine sharing data with advertisers or government. In addition, assessment and audits most commonly evaluate technology companies against established criteria, such as international human rights standards, regulatory requirements, or voluntary principles to which a company has previously committed. Accordingly, any call to increase the number or scope of assessments and audits, either voluntarily or through legal requirements, must also consider the precise services that should be assessed or audited, the procedures to be used, and the criteria a company will be evaluated against.

What information from assessments and audits should be made publicly available?

Assessments and audits can provide valuable and valid assurances of company compliance with established criteria or standards based solely on the opinion offered by the individual or entity conducting the evaluation, if the evaluator is sufficiently credible. When evaluators publish not only their final opinion but also information about how they reached their conclusion, they can also enhance the transparency of technology company practices. Some kinds of analysis, like the Ranking Digital Rights evaluations of company practice, are conducted on the basis of already-public information. But not all information obtained in the course of an assessment or audit can be published. Assessors and auditors may need access to sensitive or confidential information from companies in order to create an accurate and complete evaluation, and companies may be willing to reveal this information only if it will not be publicly disclosed.

Companies may also seek to review reports before they are published in order evaluate whether any information they contain is privileged or protected by trade secret, and to redact this information or otherwise modify the report. If assessments or audits are to serve the additional purpose of transparency, however, final reports must reveal enough information to allow the public to understand and evaluate them and hold companies

20 *ISO/IEC 17011:2017 Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies*, International Organization for Standardization (last visited Nov. 29, 2021).

responsible for the results, while not disclosing trade secrets or other proprietary information. Some assessments, like the GNI Company Assessments, try to strike this balance by providing information in anonymized or aggregate format. The competing interests in transparency and nondisclosure must be weighed against each other in determining what information and level of detail a final assessment or audit report should include.

This brief is a part of the December 2021 CDT report, *Making Transparency Meaningful: A Framework for Policymakers*.

Additional CDT work on this topic: https://cdt.org/insights/report-making-transparency-meaningful-a-framework-for-policymakers

For more info, please contact **Emma Llansó**, Director of the CDT Free Expression Project or **Caitlin Vogus**, Deputy Director of the CDT Free Expression project.

ellanso@cdt.org

@ellanso

cvogus@cdt.org

@CaitlinVogus

The **Center for Democracy & Technology** (CDT) is a 25-year-old 501(c)3 nonpartisan nonprofit organization working to promote democratic values by shaping technology policy and architecture. The organisation is headquartered in Washington, D.C. and has a Europe Office in Brussels, Belgium.

@CenDemTech

CENTER FOR DEMOCRACY & TECHNOLOGY