TECHNOLOGY & COMMUNICATIONS SECTOR

INTERNET MEDIA & SERVICES

Sustainability Accounting Standard

Sustainable Industry Classification System® (SICS®) TC-IM

Prepared by the
Sustainability Accounting Standards Board

October 2018

INDUSTRY STANDARD | VERSION 2018-10

INTERNET MEDIA & SERVICES

Sustainability Accounting Standard

About SASB

The SASB Foundation was founded in 2011 as a not-for-profit, independent standards-setting organization. The SASB Foundation's mission is to establish and maintain industry-specific standards that assist companies in disclosing financially material, decision-useful sustainability information to investors.

The SASB Foundation operates in a governance structure similar to the structure adopted by other internationally recognized bodies that set standards for disclosure to investors, including the Financial Accounting Standards Board (FASB) and the International Accounting Standards Board (IASB). This structure includes a board of directors ("the Foundation Board") and a standards-setting board ("the Standards Board" or "the SASB"). The Standards Board develops, issues, and maintains the SASB standards. The Foundation Board oversees the strategy, finances and operations of the entire organization, and appoints the members of the Standards Board.

The Foundation Board is not involved in setting standards, but is responsible for overseeing the Standards Board's compliance with the organization's due process requirements. As set out in the SASB *Rules of Procedure,* the SASB's standards-setting activities are transparent and follow careful due process, including extensive consultation with companies, investors, and relevant experts.

The SASB Foundation is funded by a range of sources, including contributions from philanthropies, companies, and individuals, as well as through the sale and licensing of publications, educational materials, and other products. The SASB Foundation receives no government financing and is not affiliated with any governmental body, the FASB, the IASB, or any other financial accounting standards-setting body.

SUSTAINABILITY ACCOUNTING STANDARDS BOARD

1045 Sansome Street, Suite 450
San Francisco, CA 94111
415.830.9220
info@sasb.org
sasb.org

Table of Contents

INTRODUCTION

Purpose of SASB Standards

The SASB's use of the term "sustainability" refers to corporate activities that maintain or enhance the ability of the company to create value over the long term. Sustainability accounting reflects the governance and management of a company's environmental and social impacts arising from production of goods and services, as well as its governance and management of the environmental and social capitals necessary to create long-term value. The SASB also refers to sustainability as "ESG" (environmental, social, and governance), though traditional corporate governance issues such as board composition are not included within the scope of the SASB's standards-setting activities.

SASB standards are designed to identify a minimum set of sustainability issues most likely to impact the operating performance or financial condition of the typical company in an industry, regardless of location. SASB standards are designed to enable communications on corporate performance on industry-level sustainability issues in a cost-effective and decision-useful manner using existing disclosure and reporting mechanisms.

Businesses can use the SASB standards to better identify, manage, and communicate to investors sustainability information that is financially material. Use of the standards can benefit businesses by improving transparency, risk management, and performance. SASB standards can help investors by encouraging reporting that is comparable, consistent, and financially material, thereby enabling investors to make better investment and voting decisions.

Overview of SASB Standards

The SASB has developed a set of 77 industry-specific sustainability accounting standards ("SASB standards" or "industry standards"), categorized pursuant to SASB's Sustainable Industry Classification System® (SICS®). Each SASB standard describes the industry that is the subject of the standard, including any assumptions about the predominant business model and industry segments that are included. SASB standards include:

1. **Disclosure topics** – A minimum set of industry-specific disclosure topics reasonably likely to constitute material information, and a brief description of how management or mismanagement of each topic may affect value creation.

2. **Accounting metrics** – A set of quantitative and/or qualitative accounting metrics intended to measure performance on each topic.

3. **Technical protocols** – Each accounting metric is accompanied by a technical protocol that provides guidance on definitions, scope, implementation, compilation, and presentation, all of which are intended to constitute suitable criteria for third-party assurance.

4. **Activity metrics** – A set of metrics that quantify the scale of a company's business and are intended for use in conjunction with accounting metrics to normalize data and facilitate comparison.

Furthermore, the *SASB Standards Application Guidance* establishes guidance applicable to the use of all industry standards and is considered part of the standards. Unless otherwise specified in the technical protocols contained in the industry standards, the guidance in the SASB Standards Application Guidance applies to the definitions, scope, implementation, compilation, and presentation of the metrics in the industry standards.

The *SASB Conceptual Framework* sets out the basic concepts, principles, definitions, and objectives that guide the Standards Board in its approach to setting standards for sustainability accounting. The *SASB Rules of Procedure* is focused on the governance processes and practices for standards setting.

Use of the Standards

SASB standards are intended for use in communications to investors regarding sustainability issues that are likely to impact corporate ability to create value over the long term. Use of SASB standards is voluntary. A company determines which standard(s) is relevant to the company, which disclosure topics are financially material to its business, and which associated metrics to report, taking relevant legal requirements into account[1]. In general, a company would use the SASB standard specific to its primary industry as identified in SICS® . However, companies with substantial business in multiple SICS® industries can consider reporting on these additional SASB industry standards.

It is up to a company to determine the means by which it reports SASB information to investors. One benefit of using SASB standards may be achieving regulatory compliance in some markets. Other investor communications using SASB information could be sustainability reports, integrated reports, websites, or annual reports to shareholders. There is no guarantee that SASB standards address all financially material sustainability risks or opportunities unique to a company's business model.

Industry Description

The Internet Media & Services industry consists of two main segments. The Internet Media segment includes companies providing search engines and internet advertising channels, online gaming, and online communities such as social networks, as well as content, usually easily searchable, such as educational, medical, health, sports, or news content. The Internet-based Services segment includes companies selling services mainly through the Internet. The industry generates revenues primarily from online advertising, on usually free content, with other sources of revenue being subscription fees, content sales, or sale of user information to interested third parties.

[1] **Legal Note**: SASB standards are not intended to, and indeed cannot, replace any legal or regulatory requirements that may be applicable to a reporting entity's operations.

SUSTAINABILITY DISCLOSURE TOPICS & ACCOUNTING METRICS

Table 1. Sustainability Disclosure Topics & Accounting Metrics

TOPIC	ACCOUNTING METRIC	CATEGORY	UNIT OF MEASURE	CODE
Environmental Footprint of Hardware Infrastructure	(1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable	Quantitative	Gigajoules (GJ), Percentage (%)	TC-IM-130a.1
	(1) Total water withdrawn, (2) total water consumed, percentage of each in regions with High or Extremely High Baseline Water Stress	Quantitative	Thousand cubic meters (m^3), Percentage (%)	TC-IM-130a.2
	Discussion of the integration of environmental considerations into strategic planning for data center needs	Discussion and Analysis	n/a	TC-IM-130a.3
Data Privacy, Advertising Standards & Freedom of Expression	Description of policies and practices relating to behavioral advertising and user privacy	Discussion and Analysis	n/a	TC-IM-220a.1
	Number of users whose information is used for secondary purposes	Quantitative	Number	TC-IM-220a.2
	Total amount of monetary losses as a result of legal proceedings associated with user privacy[2]	Quantitative	Reporting currency	TC-IM-220a.3
	(1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure	Quantitative	Number, Percentage (%)	TC-IM-220a.4
	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring[3]	Discussion and Analysis	n/a	TC-IM-220a.5
	Number of government requests to remove content, percentage compliance with requests	Quantitative	Number, Percentage (%)	TC-IM-220a.6
Data Security	(1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of users affected [4]	Quantitative	Number, Percentage (%)	TC-IM-230a.1
	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	Discussion and Analysis	n/a	TC-IM-230a.2
Employee Recruitment, Inclusion &	Percentage of employees that are foreign nationals [5]	Quantitative	Percentage (%)	TC-IM-330a.1
	Employee engagement as a percentage[6]	Quantitative	Percentage (%)	TC-IM-330a.2

[2] Note to **TC-IM-220a.3** – The entity shall briefly describe the nature, context, and any corrective actions taken as a result of the monetary losses.
[3] Note to **TC-IM-220a.5** – Disclosure shall include a description of the extent of the impact in each case and, where relevant, a discussion of the entity's policies and practices related to freedom of expression.
[4] Note to **TC-IM-230a.1** – Disclosure shall include a description of corrective actions implemented in response to data breaches.
[5] Note to **TC-IM-330a.1** – Disclosure shall include a description of potential risks of recruiting foreign nationals and management approach to addressing these risks.
[6] Note to **TC-IM-330a.2** – Disclosure shall include a description of methodology employed.

TOPIC	ACCOUNTING METRIC	CATEGORY	UNIT OF MEASURE	CODE
Performance	Percentage of gender and racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees[7]	Quantitative	Percentage (%)	TC-IM-330a.3
Intellectual Property Protection & Competitive Behavior	Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behavior regulations[8]	Quantitative	Reporting currency	TC-IM-520a.1

Table 2. Activity Metrics

ACTIVITY METRIC	CATEGORY	UNIT OF MEASURE	CODE
Entity-defined measure of user activity[9]	Quantitative	See note	TC-IM-000.A
(1) Data processing capacity, (2) percentage outsourced[10]	Quantitative	See note	TC-IM-000.B
(1) Amount of data storage, (2) percentage outsourced[11]	Quantitative	Petabytes, Percentage (%)	TC-IM-000.C

[7] Note to **TC-IM-330a.3** – The entity shall discuss its policies and programs for fostering equitable employee representation across its global operations.

[8] Note to **TC-IM-520a.1** – The entity shall briefly describe the nature, context, and any corrective actions taken as a result of the monetary losses.

[9] Note to **TC-IM-000.A** – The entity shall define and disclose a basic measure of customer activity suitable for its business activities. This may include, but is not limited to, sales transactions, purchase transactions, number of searches, monthly active users, or page views.

[10] Note to **TC-IM-000.B** – Data processing capacity shall be reported in units of measure typically tracked by the entity or used as the basis for contracting software and IT services, such as Million Service Units (MSUs), Million Instructions per Second (MIPS), Mega FloatingPoint Operations per Second (MFLOPS), compute cycles, or other. Alternatively, the entity may disclose owned and outsourced data processing needs in other units of measure, such as rack space or data center square footage. The percentage outsourced shall include On-Premise cloud services, those that are hosted on Public Cloud, and those that are residing in Colocation Data Centers.

[11] Note to **TC-IM-000.C** – The percentage outsourced shall include On-Premise cloud services, those that are hosted on Public Cloud, and those that are residing in Colocation Data Centers.

Environmental Footprint of Hardware Infrastructure

Topic Summary

With the Internet & Media Services industry providing a growing amount of content and service offerings, companies in this industry increasingly own, operate, or rent more data centers and other hardware. Thus, the management of the energy and water use associated with IT hardware infrastructure is of great importance to shareholder value. Data centers need to be powered continuously. Disruptions to the energy supply can have a material impact on operations, depending on the magnitude and timing of the disruption. Companies face a trade-off between energy and water consumption due to data center cooling needs. Cooling data centers with water instead of chillers is a means of improving energy efficiency, but it can lead to dependence on significant local water resources. Decisions about data center specifications are important for managing costs, obtaining a reliable supply of energy and water, and lowering reputational risks, particularly as there is an increasing global regulatory focus on climate change and as opportunities arise from innovations in energy efficiency and renewable energy.

Accounting Metrics

TC-IM-130a.1. (1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable

1 The entity shall disclose (1) the total amount of energy it consumed as an aggregate figure, in gigajoules (GJ).

1.1 The scope of energy consumption includes energy from all sources, including energy purchased from sources external to the entity and energy produced by the entity itself (self-generated). For example, direct fuel usage, purchased electricity, and heating, cooling, and steam energy are all included within the scope of energy consumption.

1.2 The scope of energy consumption includes only energy directly consumed by the entity during the reporting period.

1.3 In calculating energy consumption from fuels and biofuels, the entity shall use higher heating values (HHV), also known as gross calorific values (GCV), which are directly measured or taken from the Intergovernmental Panel on Climate Change (IPCC), the U.S. Department of Energy (DOE), or the U.S. Energy Information Administration (EIA).

2 The entity shall disclose (2) the percentage of energy it consumed that was supplied from grid electricity.

2.1 The percentage shall be calculated as purchased grid electricity consumption divided by total energy consumption.

3 The entity shall disclose (3) the percentage of energy it consumed that is renewable energy.

3.1 Renewable energy is defined as energy from sources that are replenished at a rate greater than or equal to their rate of depletion, such as geothermal, wind, solar, hydro, and biomass.

3.2 The percentage shall be calculated as renewable energy consumption divided by total energy consumption.

3.3 The scope of renewable energy includes renewable fuel the entity consumed, renewable energy the entity directly produced, and renewable energy the entity purchased, if purchased through a renewable power purchase agreement (PPA) that explicitly includes renewable energy certificates (RECs) or Guarantees of Origin (GOs), a Green-e Energy Certified utility or supplier program, or other green power products that explicitly include RECs or GOs, or for which Green-e Energy Certified RECs are paired with grid electricity.

3.3.1 For any renewable electricity generated on-site, any RECs and GOs must be retained (i.e., not sold) and retired or cancelled on behalf of the entity in order for the entity to claim them as renewable energy.

3.3.2 For renewable PPAs and green power products, the agreement must explicitly include and convey that RECs and GOs be retained or replaced and retired or cancelled on behalf of the entity in order for the entity to claim them as renewable energy.

3.3.3 The renewable portion of the electricity grid mix that is outside of the control or influence of the entity is excluded from the scope of renewable energy.

3.4 For the purposes of this disclosure, the scope of renewable energy from hydro and biomass sources is limited to the following:

3.4.1 Energy from hydro sources is limited to those that are certified by the Low Impact Hydropower Institute or that are eligible for a state Renewable Portfolio Standard;

3.4.2 Energy from biomass sources is limited to materials certified to a third-party standard (e.g., Forest Stewardship Council, Sustainable Forest Initiative, Programme for the Endorsement of Forest Certification, or American Tree Farm System), materials considered eligible sources of supply according to the *Green-e Framework for Renewable Energy Certification, Version 1.0* (2017) or Green-e regional standards, and/or materials that are eligible for an applicable state renewable portfolio standard.

4 The entity shall apply conversion factors consistently for all data reported under this disclosure, such as the use of HHVs for fuel usage (including biofuels) and conversion of kilowatt hours (kWh) to GJ (for energy data including electricity from solar or wind energy).

5 The entity may disclose the trailing twelve-month (TTM) weighted average power usage effectiveness (PUE) for its data centers.

5.1 PUE is defined as the ratio of the total amount of power used by a computer data center facility to the amount of power delivered to computing equipment.

5.2 If disclosing PUE, the entity shall follow the guidance and calculation methodology described in *PUE™: A Comprehensive Examination of the Metric* (2014), published by ASHRAE and The Green Grid Association.

TC-IM-130a.2. (1) Total water withdrawn, (2) total water consumed, percentage of each in regions with High or Extremely High Baseline Water Stress

1 The entity shall disclose the amount of water, in thousands of cubic meters, that was withdrawn from all sources.

1.1 Water sources include surface water (including water from wetlands, rivers, lakes, and oceans), groundwater, rainwater collected directly and stored by the entity, and water and wastewater obtained from municipal water supplies, water utilities, or other entities.

2 The entity may disclose portions of its supply by source if, for example, significant portions of withdrawals are from non-freshwater sources.

2.1 Fresh water may be defined according to the local laws and regulations where the entity operates. Where there is no legal definition, fresh water shall be considered to be water that has less than 1,000 parts per million of dissolved solids per the U.S. Geological Survey.

2.2 Water obtained from a water utility in compliance with U.S. National Primary Drinking Water Regulations can be assumed to meet the definition of fresh water.

3 The entity shall disclose the amount of water, in thousands of cubic meters, that was consumed in its operations.

3.1 Water consumption is defined as:

3.1.1 Water that evaporates during withdrawal, usage, and discharge;

3.1.2 Water that is directly or indirectly incorporated into the entity's product or service;

3.1.3 Water that does not otherwise return to the same catchment area from which it was withdrawn, such as water returned to another catchment area or the sea.

4 The entity shall analyze all of its operations for water risks and identify activities that withdraw and consume water in locations with High (40–80 percent) or Extremely High (>80 percent) Baseline Water Stress as classified by the World Resources Institute's (WRI) Water Risk Atlas tool, Aqueduct.

5 The entity shall disclose its water withdrawn in locations with High or Extremely High Baseline Water Stress as a percentage of the total water withdrawn.

6 The entity shall disclose its water consumed in locations with High or Extremely High Baseline Water Stress as a percentage of the total water consumed.

TC-IM-130a.3. Discussion of the integration of environmental considerations into strategic planning for data center needs

1 The entity shall describe its approach to the integration of environmental considerations, including energy and water use, into strategic planning for data centers.

2 Discussion shall include, but is not limited to, how environmental factors impact the entity's decisions regarding the siting, design, construction, refurbishment, and operations of data centers.

2.1 Environmental factors and criteria may include, but are not limited to:

2.1.1 Location-based environmental factors, such as regional humidity, average temperature, and water availability.

2.1.2 Environmental regulations, such as energy efficiency standards and national- or state-level carbon legislation on pricing, and carbon intensity of grid electricity.

3 The scope of disclosure includes considerations for existing owned data centers, development of new data centers, and outsourcing of data center services, where relevant.

Data Privacy, Advertising Standards & Freedom of Expression

Topic Summary

Companies in the Internet & Media Services industry rely on customer data to innovate new tools and services, generate revenues through advertising sales, and track and prevent criminal activities, such as hacking and online predators targeting children. However, the use and storage of a wide range of customer data, such as personal, demographic, content, and behavioral data, raises privacy concerns, leading to increased regulatory scrutiny in many countries around the world. Companies face reputational risks from providing access to user data to governments, which raises concerns that the data may be used to limit the freedoms of citizens. Companies may also face increased costs of compliance associated with the varying local laws or government demands related to censorship of culturally or politically sensitive material on websites. This issue has impacts on company profitability through the loss of users and can influence decisions to enter or operate in certain markets.

Accounting Metrics

TC-IM-220a.1. Description of policies and practices relating to behavioral advertising and user privacy

1 The entity shall describe the nature, scope, and implementation of its policies and practices related to user privacy, with a specific focus on how it addresses the collection, usage, and retention of user information.

1.1 User information includes information that pertains to a user's attributes or actions, including but not limited to, account statements, transaction records, records of communications, content of communications, demographic data, behavioral data, location data, and/or personally identifiable information (PII).

1.2 Demographic data are defined as the quantifiable statistics that identify and distinguish a given population. Examples of demographic data include gender, age, race/ethnicity, knowledge of languages, disabilities, mobility, home ownership, and employment status.

1.3 Behavioral data are defined as the product of tracking, measuring, and recording individual behaviors, such as online browsing patterns, buying habits, brand preferences, and product usage patterns.

1.4 Location data are defined as data describing the physical location or movement patterns of an individual, such as Global Positioning System (GPS) coordinates or other related data that would enable identifying and tracking an individual's physical location.

1.5 PII is defined as any information about an individual that is maintained by an entity, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number (SSN), date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment

information. This definition is derived from the U.S. Government Accountability Office's Report to Congressional Requesters, *Alternatives Exist for Enhancing Protection of Personally Identifiable Information* .

2 The entity shall describe the information "lifecycle" (i.e., collection, usage, retention, processing, disclosure, and destruction of information) and how information-handling practices at each stage may affect individuals' privacy.

2.1 With respect to data collection, it may be relevant for the entity to discuss which data or types of data are collected without the consent of an individual, which require opt-in consent, and which require opt-out action from the individual.

2.2 With respect to usage of data, it may be relevant for the entity to discuss which data or types of data are used by the entity internally, and under which circumstances the entity shares, sells, rents, or otherwise distributes data or information to third parties.

2.3 With respect to retention, it may be relevant for the entity to discuss which data or types of data it retains, the length of time of retention, and practices used to ensure that data is stored securely.

3 The entity shall discuss the degree to which its policies and practices address similar issues as those outlined in the U.S. Office of Management and Budget's "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (M-03-22)," including use of Privacy Impact Assessments (PIAs).

3.1 A PIA is an analysis of how information is handled that ensures handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; determines the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and examines and evaluates protections and alternative processes for handling information in order to mitigate potential privacy risks.

3.2 As outlined by OMB M-03-22, PIAs must analyze and describe: (a) what information is to be collected, (b) why the information is being collected, (c) the intended use of the information, (d) with whom the information will be shared, (e) what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), including how individuals can grant consent, and (f) how the information will be secured, among other government-specific requirements.

4 The entity shall discuss how its policies and practices related to privacy of user information address children's privacy, which at a minimum includes the provisions of the U.S. Children's Online Privacy Protection Act (COPPA).

5 The scope of disclosure includes both first- and third-party advertising.

6 With respect to behavioral advertising, the entity may describe how it addresses the following principles, described by the cross-industry Self-Regulatory Principles for Online Behavioral Advertising:

6.1 Education: participation in educational efforts for consumers about behavioral online advertising

6.2 Transparency: clearly disclosing information about data collection and data use practices

6.3 Consumer control: allowing users to choose whether data is collected or transferred to non-affiliates

6.4 Data security: providing basic security provisions and having clear policies relating to retention of user information

6.5 Material changes: obtaining consent before applying changes to policies that are less restrictive than existing ones

6.6 Sensitive data: abiding by COPPA, and handling user data such as financial information, Social Security numbers, and medical information

6.7 Accountability: participation in self-regulatory organizations such as the Direct Marketing Association

TC-IM-220a.2. Number of users whose information is used for secondary purposes

1 The entity shall disclose the number of unique users whose information is used for secondary purposes.

1.1 User information includes information that pertains to a user's attributes or actions, including but not limited to, account statements, transaction records, records of communications, content of communications, demographic data, behavioral data, location data, and/or personally identifiable information (PII).

1.1.1 Demographic data are defined as the quantifiable statistics that identify and distinguish a given population. Examples of demographic data include gender, age, race/ethnicity, knowledge of languages, disabilities, mobility, home ownership, and employment status.

1.1.2 Behavioral data are defined as the product of tracking, measuring, and recording individual behaviors such as online browsing patterns, buying habits, brand preferences, and product usage patterns.

1.1.3 Location data are defined as data describing the physical location or movement patterns of an individual, such as Global Positioning System (GPS) coordinates or other related data that would enable identifying and tracking an individual's physical location.

1.1.4 PII is defined as any information about an individual that is maintained by an entity, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number (SSN), date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. This definition is derived from the U.S. Government Accountability Office's Report to Congressional Requesters, *Alternatives Exist for Enhancing Protection of Personally Identifiable Information* .

1.2 Secondary purpose is defined as the intentional use of data by the entity (i.e., not a breach of security) that is outside the primary purpose for which the data was collected. Examples of secondary purposes include, but are not limited to, selling targeted ads, improving the entity's products or service offerings, and transferring data or information to a third-party through sale, rental, or sharing.

1.3 User accounts that the entity cannot verify as belonging to the same individual shall be disclosed separately.

2 The scope of disclosure shall include the users whose information is used by the entity itself for secondary purposes as well as the users whose information is provided to affiliates or non-affiliates to use for secondary purposes.

2.1 Affiliate is defined as an entity that directly or indirectly controls, is controlled by, or is under common control with the entity.

2.2 Non-affiliates are all third parties other than the entity and its affiliates.

TC-IM-220a.3. Total amount of monetary losses as a result of legal proceedings associated with user privacy

1 The entity shall disclose the total amount of monetary losses it incurred during the reporting period as a result of legal proceedings associated with incidents relating to user privacy.

2 The legal proceedings shall include any adjudicative proceeding in which the entity was involved, whether before a court, a regulator, an arbitrator, or otherwise.

3 The losses shall include all monetary liabilities to the opposing party or to others (whether as the result of settlement or verdict after trial or otherwise), including fines and other monetary liabilities incurred during the reporting period as a result of civil actions (e.g., civil judgments or settlements), regulatory proceedings (e.g., penalties, disgorgement, or restitution), and criminal actions (e.g., criminal judgment, penalties, or restitution) brought by any entity (e.g., governmental, business, or individual).

4 The scope of monetary losses shall exclude legal and other fees and expenses incurred by the entity in its defense.

5 The scope of disclosure shall include, but is not limited to, legal proceedings associated with the enforcement of relevant industry regulations, such as:

5.1 California Consumer Privacy Act

5.2 EU Directive 2002/58/EC (ePrivacy Directive)

5.3 EU-U.S. Privacy Shield

5.4 EU's General Data Protection Regulation (GDPR) (EU) 2016/679

5.5 Japan's Act on the Protection of Personal Information

5.6 U.S. Children's Online Privacy Protection Act

5.7 U.S. Federal Trade Commission Privacy Act

6 The scope of disclosure shall include, but is not limited to, legal proceedings associated with the enforcement of relevant industry regulations promulgated by regional, national, state, and local regulatory authorities, such as:

6.1 European Data Protection Supervisor

6.2 Japan's Personal Information Protection Commission

6.3 U.S. Federal Trade Commission

Note to **TC-IM-220a.3**

1 The entity shall briefly describe the nature (e.g., judgment or order issued after trial, settlement, guilty plea, deferred prosecution agreement, non-prosecution agreement) and context (e.g., unauthorized monitoring, sharing of data, children's privacy) of all monetary losses as a result of legal proceedings.

2 The entity shall describe any corrective actions it has implemented as a result of the legal proceedings. This may include, but is not limited to, specific changes in operations, management, processes, products, business partners, training, or technology.

TC-IM-220a.4. (1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure

1 The entity shall disclose (1) the total number of unique requests for user information, including user content and non-content data, from government or law enforcement agencies.

1.1 Content data includes user-generated information such as email text or recorded phone conversation.

1.2 Non-content data includes information such as an email address, a person's name, country of residence, or gender, or system-generated data such as IP addresses and traffic data.

1.3 Both content and non-content data can include personally identifiable information (PII).

1.3.1 PII is defined as any information about an individual that is maintained by an entity, including (a) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number (SSN), date and place of birth, mother's maiden name, or biometric records; and (b) any other information that is linked or linkable to an individual, such as medical, educational, financial,

and employment information. This definition is derived from the U.S. Government Accountability Office's Report to Congressional Requesters, *Alternatives Exist for Enhancing Protection of Personally Identifiable Information* .

2 The entity shall disclose (2) the total number of unique users whose information was requested by government or law enforcement agencies.

2.1 The number of records requested shall be calculated as the sum of unique users whose information was requested across all requests for information from government or law enforcement agencies received during the reporting period.

2.1.1 If the entity is not able to verify that two accounts (i.e., user information) belong to the same user, the entity shall consider this two users.

3 The entity shall disclose (3) the percentage of government and law enforcement requests that resulted in disclosure to the requesting party.

3.1 The percentage shall be calculated as the number of unique requests that resulted in disclosure to the requesting party divided by the total number of unique requests received.

3.2 The scope of requests that resulted in disclosure shall include requests that resulted in full or partial compliance with the disclosure request within the reporting period.

3.3 The scope of this requests that resulted in disclosure shall include disclosure of aggregated, de-identified, and anonymized data, which is intended to prevent the recipient from reconfiguring the data to identify an individual's actions or identity.

3.3.1 The entity may discuss whether these characteristics apply to a portion of its data releases if this discussion would provide necessary context for interpretation of the entity disclosure.

4 The entity may additionally break down its disclosure by region or country.

5 The entity may describe its policy for determining whether to comply with a request for user data, including under what conditions it will release user data, what requirements must be met in the request, and the level of management approval required.

6 The entity may describe its policy for notifying users about such requests, including the timing of notification.

TC-IM-220a.5. List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring

1 The entity shall disclose a list of the countries where its products and services are monitored, blocked, content is filtered, or censored due to governmental, judicial, or law enforcement requests or requirements, where:

1.1 Monitoring occurs when a government authority or law enforcement agency has routine access to content or non-content data of specific users or all users of a particular product or service.

1.2 Blocking occurs when the entity is prohibited by law or government authority from providing some or all of the entity's products or services in a country.

1.3 Content filtering or censoring occurs when a government authority alters access to, or display of, content of a product or service either directly by overriding service provision, or indirectly by requiring that a company remove certain content. Examples include content that is considered politically or culturally sensitive.

2 The scope of this disclosure includes company operations that have been discontinued, or were never offered, in a region due to government activity related to monitoring, blocking, content filtering, or censoring.

Note to **TC-IM-220a.5**

1 The entity shall describe the extent of monitoring, blocking, content filtering, or censorship across its product or service lines, including the specific products affected, nature and duration of impact, and percent of customers affected.

2 The entity may discuss implications of blocking or censorship, such as affecting ability to grow market share, or increased costs to comply with these restrictions.

3 For products and services that have been modified in a manner material to their functionality, the entity shall identify the product or service affected and discuss the nature of the modification, indicating whether modification was undertaken to avoid monitoring or blocking, or to enable monitoring or blocking. The entity shall describe how the modified product or service differs from the product or service offering in its home country or other significant markets.

4 Where relevant, the entity shall discuss its policies and practices related to freedom of expression, including how they influence its decision making when operating in countries that may request or require some form of monitoring, blocking, content filtering, or censoring of the entity's content.

TC-IM-220a.6. Number of government requests to remove content, percentage compliance with requests

1 The entity shall disclose the number of requests to remove content it received from government or law enforcement agencies.

1.1 The scope of content removal requests includes, but is not limited to, instances where the content is restricted in one or more markets the entity operates in, but not others.

2 The entity shall disclose the percentage of the requests from government or law enforcement agencies to remove content where the entity complied with the issuing agencies to remove content.

2.1 The entity shall calculate the percentage as the number of requests the entity complied with divided by the total number of requests to remove content the entity had received.

2.2 The scope of requests the entity complied with shall include requests that resulted in full or partial compliance with the disclosure request within the reporting period.

3 The entity may describe its policy for determining whether to comply with a request to remove content, including under what conditions it will remain, what requirements must be met in the request, and the level of management approval required.

4 The entity may break out categories of request type (e.g., copyright takedown notices, illegal hate speech).

5 The entity may provide disclosures by region or country.

Data Security

Topic Summary

Companies in the Internet Media & Services industry are subject to a large and growing number of cyber attacks and social engineering threats, which puts customer information and a company's own data at risk. Inadequate prevention, detection, and remediation of data security threats can influence customer acquisition and retention and result in decreased market share and lower demand for the company's products and/or services. By identifying and addressing data security threats in a timely manner companies can protect brand value and will be better positioned for customer acquisition and retention. Furthermore, effective management can avoid significant expenses associated with data breaches—most commonly directed at recapturing users following a breach.

Accounting Metrics

TC-IM-230a.1. (1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of users affected

1 The entity shall calculate and disclose (1) the total number of data breaches identified during the reporting period.

1.1 Data breach is defined as the unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information. This definition is derived from the U.S. National Initiative for Cybersecurity Careers and Studies (NICCS) glossary.

1.2 The scope of disclosure is limited to data breaches that resulted in a deviation from the entity's expected outcomes for confidentiality and/or integrity.

2 The entity shall disclose (2) the percentage of data breaches in which personally identifiable information (PII) was subject to the data breach.

2.1 PII is defined as any information about an individual that is maintained by an entity, including: (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number (SSN), date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. This definition is derived from the U.S. Government Accountability Office's Report to Congressional Requesters, *Alternatives Exist for Enhancing Protection of Personally Identifiable Information* .

2.2 The scope of disclosure shall include incidents in which encrypted data were acquired with an encryption key that was also acquired, as well as if there is a reasonable belief that encrypted data could be readily converted to plaintext.

2.2.1 Encryption is defined as the process of transforming plaintext into ciphertext. This definition is derived from the NICCS glossary.

2.3 The scope of disclosure is limited to breaches in which users were notified of the breach, either as required by law or voluntarily by the entity.

3 The entity shall disclose (3) the total number of unique users who were affected by data breaches, which includes all those whose personal data was compromised in a data breach.

3.1 Accounts that the entity cannot verify as belonging to the same user shall be disclosed separately.

4 The entity may delay disclosure if a law enforcement agency has determined that notification impedes a criminal investigation or until the law enforcement agency determines that such notification does not compromise the investigation.

Note to **TC-IM-230a.1**

1 The entity shall describe the corrective actions taken in response to specific incidents, such as changes in operations, management, processes, products, business partners, training, or technology.

1.1 The U.S. SEC's Commission Statement and Guidance on Public Company Cybersecurity Disclosures may provide further guidance on disclosures on the corrective actions taken in response to data breaches.

2 All disclosure shall be sufficient such that it is specific to the risks the entity faces, but disclosure itself will not compromise the entity's ability to maintain data privacy and security.

3 The entity should disclose its policy for disclosing data breaches to affected users in a timely manner.

TC-IM-230a.2. Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards

1 The entity shall describe its approach to identifying vulnerabilities in its information systems that pose a data security risk.

1.1 Vulnerability is defined as a weakness in an information system, system security procedures, internal controls, and/or implementation that could be exploited.

1.2 Data security risk is defined as any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or nations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

2 The entity shall describe its approach to addressing data security risks and vulnerabilities it has identified, including, but not limited to, operational procedures, management processes, structure of products, selection of business partners, employee training, and use of technology.

3 The entity shall describe its use of third-party cybersecurity risk management standards.

3.1 Third-party cybersecurity risk management standards are defined as standards, frameworks, and/or guidance developed by a third-party with the explicit purpose of aiding companies in identifying cybersecurity threats, and/or preventing, responding to, and/or remediating cybersecurity incidents.

3.2 Examples of third-party cybersecurity risk management standards include, but are not limited to:

3.2.1 The American Institute of Certified Public Accountants' (AICPA) Service Organization Controls (SOC) for Cybersecurity

3.2.2 ISACA's COBIT 5

3.2.3 ISO/IEC 27000-series

3.2.4 National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*

3.3 Disclosure shall include, but is not limited to:

3.3.1 Identification of the specific cybersecurity risk management standard(s) that have been implemented or are otherwise in use

3.3.2 Description of the extent of its use of cybersecurity risk management standard(s), such as by applicable operations, business unit, geography, product, or information system

3.3.3 The role of cybersecurity risk management standards in the entity's overall approach to identifying vulnerabilities in its information systems and addressing data security risks and vulnerabilities

3.3.4 If the third-party verification of the use of cybersecurity risk management standards is conducted, including independent examinations or audits

3.3.5 Ongoing activities and initiatives related to increasing the use of cybersecurity risk management standards, even if such standards are not currently in use

4 The entity may discuss trends it has observed in type, frequency, and origination of attacks to its data security and information systems.

5 The U.S. SEC's Commission Statement and Guidance on Public Company Cybersecurity Disclosures may provide further guidance on disclosures on the entity's approach to addressing data security risks and vulnerabilities.

6 All disclosure shall be sufficient such that it is specific to the risks the entity faces but disclosure itself would not compromise the entity's ability to maintain data privacy and security.

Employee Recruitment, Inclusion & Performance

Topic Summary

Employees are key contributors to value creation in the Internet Media & Services industry. While the number of job openings in the industry continues to grow, companies are finding it difficult to recruit qualified employees to fill these positions. The shortage in technically skilled domestic employees has created intense competition to acquire highly skilled employees, contributing to high employee turnover rates. In response to talent shortages, companies are hiring foreign nationals, which creates risks related to perceived social implications in the host and home countries of workers. Companies offer significant monetary and non-monetary benefits in order to improve employee engagement and, therefore, retention and productivity increase. Initiatives to improve employee engagement and work-life balance might influence the recruitment and retention of a diverse workforce. As the industry is characterized by relatively low representation from women and minority groups, efforts to recruit from and develop diverse talent pools can serve to address the talent shortage and generally to improve the value of company offerings. Greater workforce diversity is important for innovation, and it helps companies understand the needs of their diverse and global customer base.

Accounting Metrics

TC-IM-330a.1. Percentage of employees that are foreign nationals

1 The entity shall disclose the percentage of employees that are foreign nationals.

1.1 Foreign nationals are defined as anyone requiring a visa for work in the country in which he or she is employed.

1.2 The percentage shall be calculated as the number of employees that are foreign nationals divided by the total number of the entity's employees.

Note to **TC-IM-330a.1**

1 The entity shall describe potential risks from recruiting foreign nationals, which may arise from immigration, naturalization, or visa regulations.

2 The entity shall describe management's approach to addressing the risks it has identified related to recruiting foreign nationals, which may include developing local talent pools, political lobbying for immigration reform, outsourcing of operations, or joining or forming industry partnerships.

TC-IM-330a.2. Employee engagement as a percentage

1 The entity shall disclose employee engagement as a percentage.

1.1 Employee engagement levels include, but are not limited to:

1.1.1 Actively engaged

1.1.2 Not engaged

1.1.3 Passive

1.1.4 Actively disengaged

1.2 If employee engagement is measured as an index (e.g., strength of employee agreement with a survey statement), the entity shall convert the index into a percentage for this disclosure.

2 The percentage shall be calculated as the number of employees who are actively engaged divided by the total number of employees who completed the survey.

2.1 The percentage shall be calculated based on the results of an employee engagement survey or research study conducted by the entity, by an external party contracted by the entity to perform such a study, or by an independent third party.

Note to **TC-IM-330a.2**

1 The entity shall briefly describe:

1.1 The source of its survey (e.g., third-party survey or entity's own)

1.2 The methodology used to calculate the percentage

1.3 A summary of questions or statements included in the survey or study (e.g., those related to goal setting, support to achieve goals, training and development, work processes, and commitment to the organization)

2 When the survey methodology has changed compared to previous reporting years, the entity shall indicate results based on both the old and new methods for the year in which the change is made.

3 If results are limited to a subset of employees, the entity shall include the percentage of employees included in the study or survey and the representativeness of the sample.

4 The entity may disclose results of other survey findings, such as the percentage of employees who are: proud of their work/where they work, inspired by their work/co-workers, and aligned with corporate strategy and goals.

TC-IM-330a.3. Percentage of gender and racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees

1 The entity shall disclose gender representation for all employees and racial/ethnic group representation for its U.S. employees by employee category.

1.1 The following employee categories shall be used: (1) management, (2) technical staff, and (3) all other employees.

2 Gender and racial/ethnic group representation shall be disclosed in percentages, where the percentage shall be calculated as the number of employees in each gender or racial/ethnic group in each employee category divided by the total number of employees in the respective employee category.

3 For U.S. employees, the entity shall categorize the employees in accordance with the Equal Employment Opportunity Commission's Employer Information EEO-1 report (EEO-1 Survey) Instruction Booklet, where each employee category for disclosure is defined by corresponding job categories and descriptions in the Instruction Booklet:

3.1 Management includes the following:

3.1.1 Executives/Senior Level Officials and Managers: individuals who plan, direct and formulate policies, set strategy and provide the overall direction of enterprises/organizations for the development and delivery of products or services, within the parameters approved by boards of directors or other governing bodies. Residing in the highest levels of organizations, these executives plan, direct or coordinate activities with the support of subordinate executives and staff managers. They include, in larger organizations, those individuals within two reporting levels of the CEO, whose responsibilities require frequent interaction with the CEO. Examples of these kinds of managers are: chief executive officers, chief operating officers, chief financial officers, line of business heads, presidents or executive vice presidents of functional areas or operating groups, chief information officers, chief human resources officers, chief marketing officers, chief legal officers, management directors and managing partners.

3.1.2 Non-executive management includes First/Mid Level Officials and Managers: individuals who serve as managers, other than those who serve as Executive/Senior Level Officials and Managers, including those who oversee and direct the delivery of products, services or functions at group, regional or divisional levels of organizations. These managers receive directions from the Executive/Senior Level management and typically lead major business units. They implement policies, programs and directives of executive/senior management through subordinate managers and within the parameters set by Executive/Senior Level management. Examples of these kinds of managers are: vice presidents and directors, group, regional or divisional controllers; treasurers; human resources, information systems, marketing, and operations managers. The First/Mid Level Officials and Managers subcategory also includes those who report directly to middle managers. These individuals serve at functional, line of business segment or branch levels and are responsible for directing and executing the day-to-day operational objectives of enterprises/organizations, conveying the directions of higher level officials and

managers to subordinate personnel and, in some instances, directly supervising the activities of exempt and non-exempt personnel. The EEO-1 Job Classification Guide provides examples of job titles in this category.

3.2 Technical staff includes employees categorized in the 15-0000 group (Computer and Mathematical Occupations) or 17-0000 group (Architecture and Engineering Occupations) of the U.S. Bureau of Labor Statistics' 2018 Standard Occupational Classification System.

3.3 All other employees includes those employees who are not classified as management or technical staff.

4 For non-U.S. employees, the entity shall categorize the employees in a manner generally consistent with the definitions provided above, though in accordance with, and further facilitated by, any applicable local regulations, guidance, or generally accepted definitions.

5 The entity shall categorize the gender of its employees as female, male, or not disclosed/available.

6 The entity shall categorize the racial/ethnic group of its U.S. employees in accordance with the EEO-1 Survey Instruction Booklet and use the following categories: Asian, Black or African American, Hispanic or Latino, White, Other (which includes Native American or Alaska Native, Native Hawaiian or Pacific Islander, and "Two or More Races" classifications), or not disclosed/available.

7 The entity may provide supplemental disclosures on gender and/or racial/ethnic group representation by country or region.

8 The entity may provide supplemental contextual disclosures on factors that significantly influence gender and/or racial/ethnic group representation, such as the country or region where employees are located.

9 The entity may disclose gender and/or racial/ethnic group representation by employee category in the following table formats:

Table 3. Gender Representation of Global Employees (%)

	FEMALE	MALE	N/A *
Management			
Technical Staff			
All Other Employees			

* N/A = not available or not disclosed

Table 4. Racial/Ethnic Group Representation of U.S. Employees (%)

	ASIAN	BLACK OR AFRICAN AMERICAN	HISPANIC OR LATINO	WHITE	OTHER ^	N/A *
Management						
Technical Staff						
All Other Employees						

^ Other includes the classifications: Native American or Alaska Native, Native Hawaiian or Pacific Islander, and "Two or More Races"
* N/A = not available or not disclosed

Note to **TC-IM-330a.3**

1 The entity shall describe its policies and programs for fostering equitable employee representation across its global operations.

1.1 Relevant policies may include maintaining transparency of hiring, promotion, and wage practices, ensuring equal employment opportunity, developing and disseminating diversity policies, and ensuring management accountability for equitable representation.

1.2 Relevant programs may include trainings on diversity, mentorship and sponsorship programs, partnership with employee resource and advisory groups, and provision of flexible work schedules to accommodate the varying needs of employees.

1.3 Relevant aspects of employee representation include, at a minimum, gender and race/ethnicity. The entity may disclose on other aspects of its workforce, such as age, physical abilities/qualities, sexual orientation, and religious beliefs, as relevant to local jurisdiction.

Intellectual Property Protection & Competitive Behavior

Topic Summary

Despite the openness of the Internet, companies in the Internet Media & Services industry spend a significant proportion of their revenues on intellectual property (IP) protection, including acquiring patents and copyrights. While IP protection is inherent to the business model of some companies in the industry and is an important driver of innovation, the IP practices of companies can be a contentious societal issue. Companies could sometimes acquire patents and other IP protection to restrict competition and access to benefits from innovation, particularly if they are dominant market players. Due to the complexity of software, its abstract nature, and increasing IP rights protection related to software, Internet Media & Services companies have to navigate overlapping patent claims to be able to operate. As a result, companies in the industry may find themselves constantly in litigation or subject to regulatory scrutiny either due to allegations of patent violations if they engage in unethical business practices, or are perceived as doing so, or because they are suing others for IP infringement. Adverse legal or regulatory rulings related to antitrust and IP can expose internet media and services companies to costly and lengthy litigations and potential monetary losses as a result. Such rulings may also affect a company's market share and pricing power if its patents or dominant position in key markets are legally challenged, with significant impact on revenue. Therefore, companies that can balance the protection of their IP and its use to spur innovation with ensuring their IP management and other business practices do not unfairly restrict competition, have the potential to lower regulatory scrutiny and legal actions while protecting their market value.

Accounting Metrics

TC-IM-520a.1. Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behavior regulations

1 The entity shall disclose the total amount of monetary losses it incurred during the reporting period as a result of legal proceedings associated with anti-competitive behavior such as those related to enforcement of laws and regulations on price fixing, anti-trust behavior (e.g., exclusivity contracts), patent misuse, or network effects and bundling of services and products to limit competition.

2 The legal proceedings shall include any adjudicative proceeding in which the entity was involved, whether before a court, a regulator, an arbitrator, or otherwise.

3 The losses shall include all monetary liabilities to the opposing party or to others (whether as the result of settlement or verdict after trial or otherwise), including fines and other monetary liabilities incurred during the reporting period as a result of civil actions (e.g., civil judgments or settlements), regulatory proceedings (e.g., penalties, disgorgement, or restitution), and criminal actions (e.g., criminal judgment, penalties, or restitution) brought by any entity (e.g., governmental, business, or individual).

4 The scope of monetary losses shall exclude legal and other fees and expenses incurred by the entity in its defense.

5 The scope of disclosure shall include, but is not limited to, legal proceedings associated with the enforcement of relevant regulations, such as:

5.1 Articles 101 to 109 of the Treaty on the Functioning of the European Union

5.2 Japan's Act on Prohibition of Private Monopolization and Maintenance of Fair Trade

5.3 The U.S. Clayton Antitrust Act of 1914

5.4 The U.S. Federal Trade Commission Act of 1914

5.5 The U.S. Sherman Antitrust Act of 1890

6 The scope of disclosure shall include, but is not limited to, legal proceedings associated with the enforcement of relevant industry regulations promulgated by regional, national, state, and local regulatory authorities, such as:

6.1 Japan Fair Trade Commission

6.2 U.S. Federal Trade Commission

Note to **TC-IM-520a.1**

1 The entity shall briefly describe the nature (e.g., judgment or order issued after trial, settlement, guilty plea, deferred prosecution agreement, non-prosecution agreement) and context (e.g., price fixing, patent misuse, anti-trust) of all monetary losses as a result of legal proceedings.

2 The entity shall describe any corrective actions it has implemented as a result of the legal proceedings. This may include, but is not limited to, specific changes in operations, management, processes, products, business partners, training, or technology.

SUSTAINABILITY ACCOUNTING STANDARDS BOARD
1045 Sansome Street, Suite 450
San Francisco, CA 94111
415.830.9220
info@sasb.org

sasb.org