

Comparison of 2019 RDR Index indicators to the draft 2020 RDR Index indicators

In January 2019, Ranking Digital rights (RDR) began a process of expanding and revising the RDR Corporate Accountability Index methodology to include [new issue areas and new company types](#). This work has focused on three main areas:

- **Improving current methodology:** This consisted of reviewing the [2019 RDR Index methodology](#) to identify key areas for revision and improvement.
- **Incorporating new indicators on targeted advertising and algorithmic systems:** This consisted of developing new indicators that set global accountability and transparency standards for how companies can demonstrate respect for human rights online as they develop and deploy these new technologies. In October 2019, RDR published [draft indicators on targeted advertising and algorithms](#), based on nearly a year of internal research and incorporating feedback from more than 90 expert stakeholders. These draft indicators were pilot-tested by the RDR research team, the results of which were published in [March 2020](#).
- **Incorporating new companies:** In early 2019, we began the process of research and public consultation on ways to expand the RDR Index to include Amazon and Alibaba. This process has laid the groundwork for incorporating two new services—e-commerce platforms and “personal digital assistant ecosystems”—into the 2020 RDR Index methodology.

This table summarizes the key revisions introduced to the 2020 RDR Index methodology as a result of our work in these three areas. It is designed to help stakeholders view the [2019 RDR Index methodology](#) in comparison to the draft version of the [2020 RDR Index](#). The left column presents the text of the indicators from the 2019 RDR Index methodology, and the right column presents the draft indicators we have proposed for the 2020 RDR Index methodology.

We encourage stakeholders to review the following documents for additional detail on the changes we are proposing.

- [A summary of the proposed revisions to the RDR research methodology](#)
- [The draft version of the 2020 RDR Index methodology](#)

We invite feedback on the proposed revisions through **Friday, May 15, 2020**. Comments should be sent via email to methodology@rankingdigitalrights.org.

In the table below, the **red** text indicates revisions to the 2019 RDR Index methodology. New draft indicators and elements are marked in **blue**. These revisions also incorporate draft indicators that were introduced in October 2019 and then pilot tested. Terms in **bold** are defined in the Glossary, which is appended in the [draft version of the 2020 RDR Index methodology](#).

2019 RDR Index methodology		DRAFT 2020 RDR Index methodology	
G1	Policy Commitment The company should publicly commit to respect users' human rights to freedom of expression and privacy.	G1	Policy Commitment The company should publish a formal policy commitment publicly commit to respect users' human rights to freedom of expression and information and privacy.
G1.1	Does the company make an explicit, clearly articulated policy commitment to human rights?	G1.1	Does the company make an explicit , clearly articulated policy commitment to human rights, including to freedom of expression and information and privacy ?
		G1.2	Does the company make an explicit, clearly articulated policy commitment to human rights, including to privacy?
		G1.3	Does the company disclose an explicit , clearly articulated policy commitment to human rights in its development and use of algorithmic systems ?
G2	Governance and management oversight	G2	Governance and management oversight

	The company's senior leadership should exercise oversight over how its policies and practices affect freedom of expression and privacy.		The company's senior leadership should exercise oversight over how its policies and practices affect freedom of expression and information , and privacy.
G2.1	Does the company clearly disclose that the board of directors exercises formal oversight over how company practices affect freedom of expression and privacy?	G2.1	Does the company clearly disclose that the board of directors exercises formal oversight over how company practices affect freedom of expression and information and privacy ?
		G2.2	Does the company clearly disclose that the board of directors exercises formal oversight over how company practices affect privacy?
G2.2	Does the company clearly disclose that an executive-level committee, team , program , or officer oversees how company practices affect freedom of expression and privacy?	G2.3	Does the company clearly disclose that an executive-level committee, team, program or officer oversees how company practices affect freedom of expression and information and privacy ?
		G2.4	Does the company clearly disclose that an executive-level committee, team, program or officer oversees how company practices affect privacy?
G2.3	Does the company clearly disclose that a management-level committee, team , program , or officer oversees how company practices affect freedom of expression and privacy?	G2.5	Does the company clearly disclose that a management-level committee, team, program or officer oversees how company practices affect freedom of expression and information and privacy ?
		G2.6	Does the company clearly disclose that a management-level committee, team, program or officer oversees how company practices affect privacy?

G3	Internal implementation The company should have mechanisms in place to implement its commitments to freedom of expression and privacy within the company.	G3	Internal implementation The company should have mechanisms in place to implement its commitments to freedom of expression and information and privacy within the company.
G3.1	Does the company clearly disclose that it provides employee training on freedom of expression and privacy issues?	G3.1	Does the company clearly disclose that it provides employee training on freedom of expression and information and privacy issues?
		G3.2	Does the company clearly disclose that it provides employee training on privacy issues?
G3.2	Does the company clearly disclose that it maintains an employee whistleblower program through which employees can report concerns related to how the company treats its users' freedom of expression and privacy rights?	G3.3	Does the company clearly disclose that it maintains an employee whistleblower program through which employees can report concerns related to how the company treats its users' freedom of expression and information and privacy rights?
		G3.4	Does the company clearly disclose that it maintains an employee whistleblower program through which employees can report concerns related to how the company treats its users' privacy rights ?
G4	Impact assessment The company should conduct regular, comprehensive, and credible due diligence, such as human rights impact assessments, to identify how all aspects of its business affect freedom of expression and privacy and to mitigate any risks posed by those impacts.	G4(a)	Impact assessment: Governments and regulations The company should conduct regular, comprehensive, and credible due diligence, through robust human rights impact assessments , to identify how government regulations and policies all aspects of its business affect freedom of expression and information and privacy, and to mitigate any risks posed by those impacts in the jurisdictions in which it operates.

G4.1	As part of its decision-making, does the company consider how laws affect freedom of expression and privacy in jurisdictions where it operates?	G4(a).1	As part of its decision-making, d Does the company consider how laws affect freedom of expression and information and privacy in jurisdictions where it operates?
		G4(a).2	Does the company consider how laws affect privacy in jurisdictions where it operates?
G4.2	Does the company regularly assess freedom of expression and privacy risks associated with existing products and services?	G4(a).3	Does the company regularly assess freedom of expression and information and privacy risks associated with existing products and services in jurisdictions where it operates?
		G4(a).4	Does the company assess privacy risks associated with existing products and services in jurisdictions where it operates?
G4.3	Does the company assess freedom of expression and privacy risks associated with a new activity, including the launch and/or acquisition of new products, services, or companies or entry into new markets?	G4(a).5	Does the company assess freedom of expression and information and privacy risks associated with a new activity, including the launch and/or acquisition of new products, services, or companies, or entry into new markets or jurisdictions?
		G4(a).6	Does the company assess privacy risks associated with a new activity, including the launch and/or acquisition of new products, services, or companies, or entry into new markets or jurisdictions?
G4.4	Does the company assess freedom of expression and privacy risks associated with the processes and mechanisms used to enforce its terms of service ?	G4(a).7	Does the company assess freedom of expression and privacy risks associated with the processes and mechanisms used to enforce its terms of service (ToS)?

G4.5	Does the company disclose that it assesses freedom of expression and privacy risks associated with its use of automated decision-making , such as through the use of algorithms and/or artificial intelligence ?	G4(a).8	Does the company assess freedom of expression and privacy risks associated with its targeted advertising policies and practices?
G4.6	Does the company assess freedom of expression and privacy risks associated with its targeted advertising policies and practices?	G4(a).9	Does the company disclose that it assesses freedom of expression and privacy risks associated with its use of automated decision-making, such as through the use of algorithms and/or artificial intelligence?
G4.7	Does the company conduct additional evaluation wherever the company's risk assessments identify concerns?	G4(a).7	Does the company disclose that it conducts additional evaluation whenever the company's risk assessments identify concerns?
G4.8	Do senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in their decision-making?	G4(a).8	Does the company disclose that senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in their decision-making?
G4.9	Does the company conduct assessments on a regular schedule?	G4(a).9	Does the company conduct assessments on a regular schedule?
G4.10	Are the company's assessments assured by an external third party ?	G4(a).10	Are the company's assessments assured by an external third party ?

G4.11	Is the external third party that assures the assessment accredited to a relevant and reputable human rights standard by a credible organization?		G4(a).11	Is the external third party that assures the assessment accredited to a relevant and reputable human rights standard by a credible organization?
			G4(b).	Impact assessment: Processes for policy enforcement The company should conduct regular, comprehensive, and credible due diligence, such as through robust human rights impact assessments , to identify how its processes for policy enforcement affect users' fundamental rights to freedom of expression and information, to privacy, and to non-discrimination, and to mitigate any risks posed by those impacts.
			G4(b).1	Does the company clearly disclose that it assesses freedom of expression and information risks of enforcing its terms of service?
			G4(b).2	Does the company clearly disclose it conducts risk assessments of its enforcement of its privacy policies?
			G4(b).3	Does the company clearly disclose that it assesses discrimination risks associated with its processes for enforcing its terms of service ?
			G4(b).4	Does the company disclose that it assesses discrimination risks associated with its processes for enforcing its privacy policies ?
			G4(b).5	Does the company conduct additional evaluation whenever the company's risk assessments identify concerns?

		G4(b).6	Do senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in their decision-making?
		G4(b).7	Does the company conduct assessments on a regular schedule?
		G4(b).8	Are the company's assessments assured by an external third party ?
		G4(b).9	Is the external third party that assures the assessment accredited to a relevant and reputable human rights standard by a credible organization?
		G4(c)	Impact assessment: Targeted advertising The company should conduct regular, comprehensive, and credible due diligence, such as through robust human rights impact assessments , to identify how all aspects of its targeted advertising policies and practices affect users' fundamental rights to freedom of expression and information, to privacy, and to non-discrimination, and to mitigate any risks posed by those impacts.
		G4(c).1	Does the company disclose that it assesses freedom of expression and information risks associated with its targeted advertising policies and practices?
		G4(c).2	Does the company disclose that it assesses privacy risks associated with its targeted advertising policies and practices?

		G4(c).3	Does the company disclose that it assesses discrimination risks associated with its targeted advertising policies and practices?
		G4(c).4	Does the company conduct additional evaluation whenever the company's risk assessments identify concerns?
		G4(c).5	Do senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in their decision-making?
		G4(c).6	Does the company conduct assessments on a regular schedule?
		G4(c).7	Are the company's assessments assured by an external third party ?
		G4(c).8	Is the external third party that assures the assessment accredited to a relevant and reputable human rights standard by a credible organization?
		G4(d)	<p>Impact assessment: Algorithmic decision-making systems.</p> <p>The company should conduct regular, comprehensive, and credible due diligence, such as through robust human rights impact assessments, to identify how all aspects of its policies and practices related to the development and use of algorithmic decision-making systems affect users' fundamental rights to freedom of expression and information, to privacy, and to</p>

			non-discrimination, and to mitigate any risks posed by those impacts.
		G4(d).1	Does the company disclose that it assesses freedom of expression and information risks associated with its development and use of algorithmic decision-making systems ?
		G4(d).2	Does the company disclose that it assesses privacy risks associated with its development and use of algorithmic decision-making systems ?
		G4(d).3	Does the company disclose that it assesses discrimination risks associated with its development and use of algorithmic decision-making systems ?
		G4(d).4	Does the company conduct additional evaluation whenever the company's risk assessments identify concerns?
		G4(d).5	Do senior executives and/or members of the company's board of directors review and consider the results of assessments and due diligence in their decision-making?
		G4(d).6	Does the company conduct assessments on a regular schedule?
		G4(d).7	Are the company's assessments assured by an external third party ?

		G4(d).8	Is the external third party that assures the assessment accredited to a relevant and reputable human rights standard by a credible organization?
		G4(e)	<p>Impact assessment: Zero-rating</p> <p>If the company engages in zero-rating, it should conduct regular, comprehensive, and credible due diligence, such as through robust human rights impact assessments, to identify how all aspects of its zero-rating policies and practices affect users' fundamental rights to freedom of expression and information, to privacy, and to freedom from discrimination, and to mitigate any risks posed by those impacts.</p>
		G4(e).1	Does the company clearly disclose that it assesses freedom of expression and information risks associated with its zero-rating programs?
		G4(e).2	Does the company clearly disclose that it assesses privacy risks associated with its zero-rating programs?
		G4(e).3	Does the company clearly disclose that it assesses discrimination risks associated with its zero-rating programs?
		G4(e).4	Does the company conduct additional evaluation wherever the company's risk assessments identify concerns?
		G4(e).5	Do senior executives and/or members of the company's board of directors review and consider the

			results of assessments and due diligence in their decision-making?
		G4(e).6	Does the company conduct assessments on a regular schedule?
		G4ed).7	Are the company's assessments assured by an external third party ?
		G4(e).8	Is the external third party that assures the assessment accredited to a relevant and reputable human rights standard by a credible organization?
G5	Stakeholder engagement The company should engage with a range of stakeholders on freedom of expression and privacy issues.	G5	Stakeholder engagement and accountability The company should engage with a range of stakeholders on the company's impact on freedom of expression and information , and privacy, and potential risks of related human rights harms such as discrimination .
G5.1	Is the company a member of a multi-stakeholder initiative whose focus includes a commitment to uphold freedom of expression and privacy based on international human rights principles?	G5.1	Is the company a member of one or more multi-stakeholder initiatives that address the full range of ways in which freedom of expression and information, privacy, and related human rights may be affected in the course of the company's operations? based on international human rights principles?
G5.2	If the company is not a member of a multi-stakeholder initiative , is the company a member of an organization that engages systematically and on a regular basis with non-industry and non-governmental stakeholders on freedom of expression and privacy?	G5.2	If the company is not a member of one or more such multi-stakeholder initiatives , is the company a member of any organizations that engages systematically and on a regular basis with non-industry

			and non-governmental stakeholders on freedom of expression and privacy?
G5.3	If the company is not a member of one of these organizations, does the company disclose that it initiates or participates in meetings with stakeholders that represent, advocate on behalf of, or are people whose freedom of expression and privacy are directly impacted by the company's business?	G5.3	If the company is not a member of one of these organizations, does the company disclose that it initiates or participates in meetings with stakeholders that represent, advocate on behalf of, or are people whose freedom of expression and privacy are directly impacted by the company's business?
G6	Remedy: The company should have grievance and remedy mechanisms to address users' freedom of expression and privacy concerns.	G6(a)	Remedy: The company should have clear and predictable grievance and remedy mechanisms to address users' freedom of expression and privacy concerns.
G6.1	Does the company clearly disclose it has a grievance mechanism(s) enabling users to submit complaints if they feel their freedom of expression or privacy has been adversely affected by the company's policies or practices?	G6(a).1	Does the company clearly disclose it has a grievance mechanism(s) enabling users to submit complaints if they feel their freedom of expression and information rights or privacy has been adversely affected by the company's policies or practices?
		G6(a).2	Does the company clearly disclose it has a grievance mechanism(s) enabling users to submit complaints if they feel their privacy has been adversely affected by the company's policies or practices?
G6.2	Does the company clearly disclose its procedures for providing remedy for freedom of expression- or privacy-related grievances?	G6(a).3	Does the company clearly disclose its procedures for providing remedy for freedom of expression and information- or privacy-related grievances ?
		G6(a).4	Does the company clearly disclose its procedures for providing remedy for privacy-related grievances ?
G6.3	Does the company clearly disclose timeframes for its grievance and remedy procedures?	G6(a).5	Does the company clearly disclose timeframes for its grievance and remedy procedures?

G6.4	Does the company clearly disclose the number of complaints received related to freedom of expression and privacy?		G6(a).6	Does the company clearly disclose the number of complaints received related to freedom of expression and privacy?
			G6(a).7	Does the company clearly disclose the number of complaints received related to privacy?
G6.5	Does the company clearly disclose evidence that it is providing remedy for freedom of expression and privacy grievances?		G6(a).8	Does the company clearly disclose evidence that it is providing remedy for freedom of expression and privacy <u>grievances</u> ?
			G6(a).9	Does the company clearly disclose evidence that it is providing remedy for privacy <u>grievances</u> ?
			G6(b)	Process for content moderation appeals The company should offer users clear and predictable appeals mechanisms and processes for appealing content-moderation actions .
			G6(b).1	Does the company clearly disclose that it offers users the ability to appeal content-moderation actions ?
			G6(b).2	Does the company clearly disclose that it notifies the user who is affected by a content-moderation action ?
			G6(b).3	Does the company clearly disclose a timeframe for notifying affected users when it takes a content-moderation action ?
			G6(b).4	Does the company clearly disclose when appeals are not permitted?
			G6(b).5	Does the company clearly disclose its process for reviewing appeals ?

		G6(b).6	Does the company clearly disclose its timeframe for reviewing appeals ?
		G6(b).7	Does the company clearly disclose the role of humans in reviewing appeals ?
		G6(b).8	Does the company clearly disclose what role automation plays in reviewing appeals ?
		G6(b).9	Does the company clearly disclose that the affected user has an opportunity to present additional information that will be considered in the review?
		G6(b).10	Does the company clearly disclose that it provides the affected user a statement outlining the reason for its decision?
		G6(b).11	Does the company clearly disclose evidence that it is addressing content moderation appeals ?
F1	Access to terms of service The company should offer terms of service that are easy to find and easy to understand .	F1(a)	Access to terms of service The company should offer terms of service that are easy to find and easy to understand .
F1.1	Are the company's terms of service easy to find ?	F1(a).1	Are the company's terms of service easy to find ?
F1.2	Are the terms of service available in the language(s) most commonly spoken by the company's users?	F1(a).2	Are the terms of service available in the primary language(s) most commonly spoken by the company's users in the company's home jurisdiction ?
F1.3	Are the terms of service presented in an understandable manner ?	F1(a).3	Are the terms of service presented in an understandable manner ?

		F1(b)	Access to advertising content policies The company should offer advertising content policies that are easy to find and easy to understand .
		F1(b).1	Are the company's advertising content policies easy to find ?
		F1(b).2	Are the company's advertising content policies available in the primary language(s) spoken by users in the company's home jurisdiction?
		F1(b).3	Are the company's advertising content policies presented in an understandable manner ?
		F1(b).4	(For mobile ecosystems): Does the company clearly disclose that it requires apps made available through its app store to provide users with an advertising content policy ?
		F1(b).5	(For personal digital assistant ecosystems): Does the company clearly disclose that it requires skills made available through its skill store to provide users with an advertising content policy ?
		F1(c).	Access to advertising targeting policies The company should offer advertising targeting policies that are easy to find and easy to understand .
		F1(c).1	Are the company's advertising targeting policies easy to find ?

		F1(c).2	Are the advertising targeting policies available in the primary language(s) spoken by users in the company's home jurisdiction?
		F1(c).3	Are the advertising targeting policies presented in an understandable manner ?
		F1(c).4	(For mobile ecosystems): Does the company clearly disclose that it requires apps made available through its app store to provide users with an advertising targeting policy ?
		F1(c).5	(For personal digital assistant ecosystems): Does the company clearly disclose that it requires skills made available through its skill store to provide users with an advertising targeting policy ?
		F1(d).	Access to algorithmic system use policies The company should offer policies related to their use of algorithms that are easy for users to find and understand .
		F1(d).1	Are the company's algorithmic system use policies easy to find ?
		F1(d).2	Are the algorithmic system use policies available in the primary language(s) spoken by users in the company's home jurisdiction?
		F1(d).3	Are the algorithmic system use policies presented in an understandable manner ?

F2	Changes to terms of service The company should clearly disclose that it provides notice and documentation to users when it changes its terms of service .	F2(a)	Changes to terms of service The company should clearly disclose that it directly notifies provides notice and documentation to users when it changes its terms of service, prior to these changes coming into effect.
F2.1	Does the company clearly disclose that it notifies users about changes to its terms of service ?	F2(a).1	Does the company clearly disclose that it directly notifies users about all changes to its terms of service ?
F2.2	Does the company clearly disclose how it will directly notify users of changes?	F2(a).2	Does the company clearly disclose how it will directly notify users of changes?
F2.3	Does the company clearly disclose the timeframe within which it provides notification prior to changes coming into effect?	F2(a).3	Does the company clearly disclose the timeframe within which it provides directly notifies users of changes prior to these changes coming into effect?
F2.4	Does the company maintain a public archive or change log ?	F2(a).4	Does the company maintain a public archive or change log ?
		F2(b)	Changes to advertising content policies The company should clearly disclose that it directly notifies users when it changes its advertising content policies , prior to these changes coming into effect.
		F2(b).1	Does the company clearly disclose that it directly notifies users about changes to its advertising content policies ?

		F2(b).2	Does the company clearly disclose how it will directly notify users of changes?
		F2(b).3	Does the company clearly disclose the timeframe within which it directly notifies users of changes prior to these changes coming into effect?
		F2(b).4	Does the company maintain a public archive or change log ?
		F2(b).5	(For mobile ecosystems): Does the company clearly disclose that it requires apps made available through its app store to notify users when the apps change their advertising content policies ?
		F2(b).6	(For personal digital ecosystems): Does the company clearly disclose that it requires skills made available through its skills store to notify users when the skills change their advertising content policies ?
		F2(c)	Changes to advertising targeting policies The company should clearly disclose that it directly notifies users when it changes its advertising targeting policies , prior to these changes coming into effect.
		F2(c).1	Does the company clearly disclose that it directly notifies users about changes to its advertising targeting policies ?

		F2(c).2	Does the company clearly disclose how it will directly notify users of changes?
		F2(c).3	Does the company clearly disclose the timeframe within which it directly notifies users of changes prior to these changes coming into effect?
		F2(c).4	Does the company maintain a public archive or change log ?
		F2(c).5	(For mobile ecosystems): Does the company clearly disclose that it requires apps made available through its app store to directly notify users when the apps change their advertising targeting policies ?
		F2(c).6	(For personal digital ecosystems): Does the company clearly disclose that it requires skills made available through its skills store to notify users when the skills change their advertising targeting policies ?
		F2(d)	Changes to algorithmic system use policies The company should clearly disclose that it directly notifies users when it changes its algorithmic system use policies , prior to these changes coming into effect.
		F2(d).1	Does the company clearly disclose that it directly notifies users about changes to its algorithmic system use policies ?
		F2(d).2	Does the company clearly disclose how it will directly notify users of changes?

		F2(d).3	Does the company clearly disclose the timeframe within which it directly notifies users of changes prior to these changes coming into effect?
		F2(d).4	Does the company maintain a public archive or change log ?
F3	Process for terms of service enforcement The company should clearly disclose the circumstances under which it may restrict content or user accounts .	F3(a)	Process for terms of service enforcement The company should clearly disclose the circumstances under which it may restrict content or user accounts .
F3.1	Does the company clearly disclose what types of content or activities it does not permit?	F3(a).1	Does the company clearly disclose what types of content or activities it does not permit?
F3.2	Does the company clearly disclose why it may restrict a user's account ?	F3(a).2	Does the company clearly disclose why it may restrict a user's account ?
F3.3	Does the company clearly disclose information about the processes it uses to identify content or accounts that violate the company's rules?	F3(a).3	Does the company clearly disclose information about the processes it uses to identify content or accounts that violate the company's rules?
		F3(a).4	Does the company clearly disclose whether it uses algorithmic systems to flag content that might violate the company's rules?
F3.4	Does the company clearly disclose whether any government authorities receive priority consideration	F3(a).5	Does the company clearly disclose whether any government authorities receive priority consideration

	when flagging content to be restricted for violating the company's rules?		when flagging content to be restricted for violating the company's rules?
F3.5	Does the company clearly disclose whether any private entities receive priority consideration when flagging content to be restricted for violating the company's rules?	F3(a).6	Does the company clearly disclose whether any private entities receive priority consideration when flagging content to be restricted for violating the company's rules?
F3.6	Does the company clearly disclose its process for enforcing its rules?	F3(a).7	Does the company clearly disclose its process for enforcing its rules once violations are detected ?
F3.7	Does the company provide clear examples to help the user understand what the rules are and how they are enforced?	F3(a).8	Does the company provide clear examples to help the user understand what the rules are and how they are enforced.
		F3(b)	Advertising content rules and enforcement The company should clearly disclose its policies governing what types of advertising content is prohibited.
		F3(b).1	Does the company clearly disclose what types of advertising content it does not permit?
		F3(b).2	Does the company clearly disclose whether it requires all advertising content must be clearly labelled as such?
		F3(b).3	Does the company clearly disclose the processes and technologies it uses to identify advertising content or accounts that violate the company's rules?
		F3(c).	Advertising targeting rules and enforcement

			The company should clearly disclose its policies governing what type of advertising targeting is prohibited.
		F3(c).1	Does the company clearly disclose whether it enables third parties to target its users with advertising content ?
		F3(c).2	Does the company clearly disclose what types of targeting parameters are not permitted?
		F3(c).3	Does the company clearly disclose that it does not permit advertisers to target specific individuals?
		F3(c).4	Does the company clearly disclose that algorithmically generated advertising audience categories are evaluated by human reviewers before they can be used?
		F3(c).5	Does the company clearly disclose information about the processes and technologies it uses to identify advertising content or accounts that violate the company's rules?
F4.	Data about terms of service enforcement The company should clearly disclose and regularly publish data about the volume and nature of actions taken to restrict content or accounts that violate the company's rules.	F4(a)	Data about content restrictions to enforce terms of service The company should clearly disclose and regularly publish data about the volume and nature of actions taken to restrict content or accounts that violates the company's rules.
F4.1	Does the company clearly disclose data about the volume and nature of content and accounts restricted for violating the company's rules?	F4(a).1	Does the company publish clearly disclose data about the total number of pieces of content volume and nature of content and accounts restricted for violating

			the company's rules? Does the company publish data about the total number of pieces of content restricted for violating the company's rules?
		F4(a).2	Does the company publish data on the number of pieces of content restricted based on which rule was violated?
		F4(a).3	Does the company publish data on the number of pieces of content it restricted based on the method used to identify the violation?
F4.2	Does the company publish this data at least once a year?	F4(a).4	Does the company publish this data at least four times once a year?
F4.3	Can the data published by the company be exported as a structured data file?	F4(a).5	Can the data be exported as a structured data file?
		F4(b)	Data about account restrictions to enforce terms of service The company should clearly disclose and regularly publish data about the volume and nature of actions taken to restrict accounts that violate the company's rules.
		F4(b).1	Does the company publish data on the total number of accounts restricted for violating the company's own rules?
		F4(b).2	Does the company publish data on the number of accounts restricted based on which rule was violated?

		F4(b).3	Does the company publish data on the number of pieces of content restricted based on the method used to identify the violation?
		F4(b).4	Does the company publish this data at least four times a year?
		F4(b).5	Can the data be exported as a structured data file?
		F4(c)	Data about advertising content policy enforcement The company should clearly disclose and regularly publish data about the volume and nature of actions taken to restrict advertising content that violates the company's advertising content policies .
		F4(c).1	Does the company publish the total number of advertisements it restricted to enforce its advertising content policies ?
		F4(c).2	Does the company publish the number of advertisements it restricted based on which rule was violated?
		F4(c).3	Does the company publish the number of advertisements it restricted based on the method used to identify the violation?
		F4(c).4	Does the company publish this data at least four times a year?
		F4(c).5	Can the data be exported as a structured data file?
		F4(d)	Data about advertising targeting policy enforcement

			The company should clearly disclose and regularly publish data about the volume and nature of actions taken to restrict advertising content that violates the company's advertising targeting policies .
		F4(d). 1	Does the company publish the total number of pieces of advertising content it restricted to enforce its advertising targeting policies ?
		F4(d). 2	Does the company publish the number of pieces of advertising content it restricts based on which rule was violated?
		F4(d). 3	Does the company publish the number of pieces of advertising content it restricts based on the method used to identify the violation?
		F4(d). 4	Does the company publish this data at least four times a year?
		F4(d). 5	Can the data be accessed through a robust programmatic interface or exported as a structured data file ?
F5	<p>Process for responding to third-party requests for content or account restriction</p> <p>The company should clearly disclose its process for responding to government requests (including judicial orders) and private requests to remove, filter, or restrict content or accounts.</p>	F5(a).	<p>Process for responding to government third-party demands requests to restrict for content or accounts restriction</p> <p>The company should clearly disclose its process for responding to government demandsrequests (including judicial orders) and private requests to remove, filter, or restrict content or accounts.</p>

F5.1	Does the company clearly disclose its process for responding to non-judicial government requests ?	F5(a).1	Does the company clearly disclose its process for responding to non-judicial government demands requests ?
F5.2	Does the company clearly disclose its process for responding to court orders ?	F5(a).2	Does the company clearly disclose its process for responding to court orders ?
F5.3	Does the company clearly disclose its process for responding to government requests from foreign jurisdictions?	F5(a).3	Does the company clearly disclose its process for responding to government demands requests from foreign jurisdictions?
		F5(a).4	Does the company clearly disclose its process for responding to private requests?
F5.5	Do the company's explanations clearly disclose the legal basis under which it may comply with government requests ?	F5(a).4	Do the company's explanations clearly disclose the legal basis under which it may comply with government demands requests ?
		F5(a).6	Do the company's explanations clearly disclose the basis under which it may comply with private requests?
F5.7	Does the company clearly disclose that it carries out due diligence on government requests before deciding how to respond?	F5(a).5	Does the company clearly disclose that it carries out due diligence on government demands requests before deciding how to respond?
		F5(a).8	Does the company clearly disclose that it carries out due diligence on private requests before deciding how to respond?

F5.9	Does the company commit to push back on inappropriate or overbroad requests made by governments ?	F5(a).6	Does the company commit to push back on inappropriate or overbroad demands requests made by governments ?
		F5(a).7	Does the company commit to push back on inappropriate or overbroad private requests?
F5.11	Does the company provide clear guidance or examples of implementation of its process of responding to government requests ?	F5(a).7	Does the company provide clear guidance or examples of implementation of its process of responding to government demands requests ?
		F5(a).12	Does the company provide clear guidance or examples of implementation of its process of responding to private requests?
		F5(b)	Process for responding to private requests for content or account restriction The company should clearly disclose its process for responding to requests to remove, filter, or restrict content or accounts that come through private processes .
F5.4	Does the company clearly disclose its process for responding to private requests ?	F5(b). 1	Does the company clearly disclose its process for responding to private requests to remove, filter, or restrict content or accounts made through private processes?
F5.6	Do the company's explanations clearly disclose the basis under which it may comply with private requests ?	F5(b). 2	Do the company's explanations clearly disclose the basis under which it may comply with private requests made through private processes?

F5.8	Does the company clearly disclose that it carries out due diligence on private requests before deciding how to respond?	F5(b).3	Does the company clearly disclose that it carries out due diligence on private requests made through private processes before deciding how to respond?
F5.10	Does the company commit to push back on inappropriate or overbroad private requests ?	F5(b).4	Does the company commit to push back on inappropriate or overbroad private requests made through private processes ?
F5.12	Does the company provide clear guidance or examples of implementation of its process of responding to private requests ?	F5(b).5	Does the company provide clear guidance or examples of implementation of its process of responding to private requests made through private processes ?
F6.	Data about government requests for content or account restriction The company should regularly publish data about government requests (including judicial orders) to remove, filter, or restrict content or accounts .	F6.	Data about government demands requests to restrict for content and or accounts The company should regularly publish data about government demands requests (including judicial orders) to remove, filter, or restrict content and or accounts .
F6.1	Does the company break out the number of requests it receives by country?	F6.1	Does the company break out the number of <u>demands</u> requests it receives by country?
F6.2	Does the company list the number of accounts affected?	F6.2	Does the company list the number of accounts affected?
F6.3	Does the company list the number of pieces of content or URLs affected?	F6.3	Does the company list the number of pieces of content or URLs affected?

F6.4	Does the company list the types of subject matter associated with the requests it receives?	F6.4	Does the company list the types of subject matter associated with the demands requests it receives?
F6.5	Does the company list the number of requests that come from different legal authorities?	F6.5	Does the company list the number of demands requests that come from different legal authorities?
F6.6	Does the company list the number of requests it knowingly receives from government officials to restrict content or accounts through unofficial processes?	F6.6	Does the company list the number of demands requests it knowingly receives from government officials to restrict content or accounts through unofficial processes ?
F6.7	Does the company list the number of requests with which it complied?	F6.7	Does the company list the number of demands requests with which it complied?
F6.8	Does the company publish the original requests or disclose that it provides copies to a public third-party archive ?	F6.8	Does the company publish the original demands requests or disclose that it provides copies to a public third-party archive ?
F6.9	Does the company report this data at least once a year?	F6.9	Does the company report this data at least once a year?
F6.10	Can the data be exported as a structured data file?	F6.10	Can the data be exported as a structured data file?
F7	Data about private requests for content or account restriction The company should regularly publish data about private requests to remove, filter, or restrict access to content or accounts .	F7	Data about private requests for content or account restriction The company should regularly publish data about private requests to remove, filter, or restrict access to content or accounts that come through private processes .

F7.1	Does the company break out the number of requests it receives by country?	F7.1	Does the company break out the number of requests to restrict content or accounts that it receives through private processes it receives by country?
F7.2	Does the company list the number of accounts affected?	F7.2	Does the company list the number of accounts affected?
F7.3	Does the company list the number of pieces of content or URLs affected?	F7.3	Does the company list the number of pieces of content or URLs affected?
F7.4	Does the company list the reasons for removal associated with the requests it receives?	F7.4	Does the company list the reasons for removal associated with the requests it receives?
F7.5	Does the company describe the types of parties from which it receives requests?	F7.5	Does the company clearly disclose the private processes that describe the types of parties from which made it receives the requests?
F7.6	Does the company list the number of requests it complied with?	F7.6	Does the company list the number of requests it complied with?
F7.7	Does the company publish the original requests or disclose that it provides copies to a public third-party archive ?	F7.7	Does the company publish the original requests or disclose that it provides copies to a public third-party archive ?
F7.8	Does the company report this data at least once a year?	F7.8	Does the company report this data at least once a year?
F7.9	Can the data be exported as a structured data file?	F7.9	Can the data be exported as a structured data file?

F7.10	Does the company clearly disclose that its reporting covers all types of private requests that it receives?	F7.10	Does the company clearly disclose that its reporting covers all types of private -requests that it receives through private processes ?
F8	User notification about content and account restriction The company should clearly disclose that it notifies users when it restricts content or accounts .	F8	User notification about content and account restriction The company should clearly disclose that it notifies users when it restricts content or accounts .
F8.1	If the company hosts user-generated content , does the company clearly disclose that it notifies users who generated the content when it is restricted?	F8.1	If the company hosts user-generated content , does the company clearly disclose that it notifies users who generated the content when it is restricted?
F8.2	Does the company clearly disclose that it notifies users who attempt to access content that has been restricted?	F8.2	Does the company clearly disclose that it notifies users who attempt to access content that has been restricted?
F8.3	In its notification, does the company clearly disclose a reason for the content restriction (legal or otherwise)?	F8.3	In its notification, does the company clearly disclose a reason for the content restriction (legal or otherwise)?
F8.4	Does the company clearly disclose that it notifies users when it restricts their account ?	F8.4	Does the company clearly disclose that it notifies users when it restricts their account ?
F9	Network management (telecommunications companies) The company should clearly disclose that it does not prioritize , block, or delay certain types of traffic, applications , protocols , or content for any reason beyond assuring quality of service and reliability of the network.	F9	Network management (telecommunications companies) The company should clearly disclose that it does not prioritize , block, or delay certain types of traffic, applications , protocols , or content for any reason beyond assuring quality of service and reliability of the network.

F9.1	Does the company clearly disclose that it does not prioritize , block, or delay certain types of traffic, applications , protocols , or content for reasons beyond assuring quality of service and reliability of the network?	F9.1	Does the company clearly disclose a policy commitment to that it does not prioritize , block, or delay certain types of traffic, applications , protocols , or content reasons beyond assuring quality of service and reliability of the network?
		F9.2	Does the company engage in practices, such as offering zero-rating programs , that prioritize network traffic for reasons beyond assuring quality of service and reliability of the network?
F9.2	If the company does engage in these practices, does it clearly disclose its purpose for doing so?	F9.3	If the company does engage in network prioritization these practices beyond assuring quality of service and reliability of the network , does it clearly disclose its purpose for doing so?
F10.	Network shutdown (telecommunications companies) The company should clearly explain the circumstances under which it may shut down or restrict access to the network or to specific protocols , services, or applications on the network.	F10.	Network shutdown (telecommunications companies) The company should clearly disclose explain the circumstances under which it may shut down or restrict access to the network or to specific protocols , services, or applications on the network.
F10.1	Does the company clearly explain the reason(s) why it may shut down service to a particular area or group of users?	F10.1	Does the company clearly disclose explain the reason(s) why it may shut down service to a particular area or group of users?
F10.2	Does the company clearly explain why it may restrict access to specific applications or protocols (e.g., VoIP, messaging) in a particular area or to a specific group of users?	F10.2	Does the company clearly disclose explain why it may restrict access to specific applications or protocols (e.g., VoIP, messaging) in a particular area or to a specific group of users?

F10.3	Does the company clearly explain its process for responding to requests to shut down a network or restrict access to a service?	F10.3	Does the company clearly disclose explain its process for responding to government demands requests to shut down a network or restrict access to a service?
F10.4	Does the company commit to push back on requests to shut down a network or restrict access to a service ?	F10.4	Does the company clearly disclose a commitment to push back on government demands requests to shut down a network or restrict access to a service ?
F10.5	Does the company clearly disclose that it notifies users directly when it shuts down the network or restricts access to a service ?	F10.5	Does the company clearly disclose that it notifies users directly when it shut down a network or restrict access to a service ?
F10.6	Does the company list the number of network shutdown requests it receives?	F10.6	Does the company clearly disclose list the number of network shutdown demands requests it receives?
F10.7	Does the company clearly identify the specific legal authority that makes the request?	F10.7	Does the company clearly disclose clearly identify the specific legal authority that makes the demands requests ?
F10.8	Does the company list the number of requests with which it complied?	F10.8	Does the company clearly disclose list the number of government demands requests with which it complied?
F11	Identity policy The company should not require users to verify their identity with their government-issued identification , or other forms of identification that could be connected to their offline identity.	F11	Identity policy The company should not require users to verify their identity with their government-issued identification , or other forms of identification that could be connected to their offline identity.

F11.1	Does the company require users to verify their identity with their government-issued identification , or with other forms of identification that could be connected to their offline identity?	F11.1	Does the company require users to verify their identity with their government-issued identification , or with other forms of identification that could be connected to their offline identity?
		F12.	Algorithmic content curation, recommendation, and/or ranking systems Companies should clearly disclose how users' online content is curated, ranked, or recommended .
		F12.1	Does the company clearly disclose whether it uses algorithmic systems to curate, recommend, and/or rank the content that users can access through its platform?
		F12.2	Does the company clearly disclose how the algorithmic systems are deployed to curate, recommend, and/or rank content , including the variables that influence these systems?
		F12.3	Does the company clearly disclose what options users have to control the variables that the algorithmic content curation, recommendation, and/or ranking system takes into account?
		F12.4	Does the company clearly disclose whether algorithmic system are used to automatically curate, recommend, and/or rank content by default?
		F12.5	Does the company clearly disclose that users can opt in to automated content curation, recommendation, and/or ranking system ?
		F13	Automated software agents (“bots”) Companies should clearly disclose policies governing

			the use of automated software agents (“bots”) on their platforms, products and services, and how they enforce such policies.
		F13.1	Does the company clearly disclose rules governing the use of bots on its platform?
		F13.2	Does the company clearly disclose that it requires users to clearly label all content and accounts that are produced, disseminated or operated with the assistance of a bot ?
		F13.3	Does the company clearly disclose its process for enforcing its bot policy ?
		F13.4	Does the company clearly disclose data on the volume and nature of user content and accounts restricted for violating the company's bot policy ?
P1	Access to privacy policies: The company should offer privacy policies that are easy to find and easy to understand .	P1(a)	Access to privacy policies: The company should offer privacy policies that are easy to find and easy to understand .
P1.1	Are the company's privacy policies easy to find ?	P1(a).1	Are the company's privacy policies easy to find ?
P1.2	Are the privacy policies available in the language(s) most commonly spoken by the company's users?	P1(a).2	Are the privacy policies available in the primary language(s) most commonly spoken by the company's users in the company's home jurisdiction ?
P1.3	Are the policies presented in an understandable manner ?	P1(a).3	Are the policies presented in an understandable manner ?

P1.4	(For mobile ecosystems): Does the company disclose that it requires apps made available through its app store to provide users with a privacy policy?	P1(a).4	(For mobile ecosystems): Does the company disclose that it requires apps made available through its app store to provide users with a privacy policy ?
		P1(a).5	(For personal digital assistant ecosystems): Does the company disclose that it requires skills made available through its skill store to provide users with a privacy policy ?
		P1(b)	Access to algorithmic system development policies: The company should offer algorithmic system development policies that are easy to find and easy to understand .
		P1(b).1	Are the company's algorithmic system development policies easy to find ?
		P1(b).2	Are the algorithmic system development policies available in the primary language(s) spoken by users in the company's home jurisdiction?
		P1(b).3	Are the algorithmic system development policies presented in an understandable manner ?
P2	Changes to privacy policies The company should clearly disclose that it provides notice and documentation to users when it changes its privacy policies.	P2(a)	Changes to privacy policies The company should clearly disclose that it directly notifies provides notice and documentation to users when it changes its privacy policies, prior to these changes coming into effect .

P2.1	Does the company clearly disclose that it notifies users about changes to its privacy policies?	P2(a).1	Does the company clearly disclose that it directly notifies users about all changes to its privacy policies ?
P2.2	Does the company clearly disclose how it will directly notify users of changes?	P2(a).2	Does the company clearly disclose how it will directly notify users of changes?
P2.3	Does the company clearly disclose the time frame within which it provides notification prior to changes coming into effect?	P2(a).3	Does the company clearly disclose the timeframe within which it provides directly notifies users of changes prior to these changes coming into effect?
P2.4	Does the company maintain a public archive or change log ?	P2(a).4	Does the company maintain a public archive or change log ?
P2.5	(For mobile ecosystems): Does the company clearly disclose that it requires apps sold through its app store to notify users when the app changes its privacy policy?	P2(a).5	(For mobile ecosystems): Does the company clearly disclose that it requires apps sold through its app store to notify users when the app changes its privacy policy ?
		P2(a).6	(For personal digital assistant ecosystems): Does the company clearly disclose that it requires skills sold through its skill store to notify users when the skill changes its privacy policy ?
P3	Collection of user information The company should clearly disclose what user information it collects and how.	P3(a)	Collection of user information The company should clearly disclose what user information it collects and how.
P3.1	Does the company clearly disclose what types of user information it collects ?	P3(a).1	Does the company clearly disclose what types of user information it collects ?

P3.2	For each type of user information the company collects , does the company clearly disclose how it collects that user information?	P3(a).2	For each type of user information the company collects , does the company clearly disclose how it collects that user information?
P3.3	Does the company clearly disclose that it limits collection of user information to what is directly relevant and necessary to accomplish the purpose of its service?	P3(a).3	Does the company clearly disclose that it limits collection of user information to what is directly relevant and necessary to accomplish the purpose of its service?
P3.4	(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose what user information the apps collect?	P3(a).4	(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose what user information the apps collects ?
P3.5	(For mobile ecosystems): Does the company clearly disclose that it evaluates whether third-party apps made available through its app store limit collection of user information to what is directly relevant and necessary to accomplish the purpose of the app?	P3(a).5	(For mobile ecosystems): Does the company clearly disclose that it evaluates whether third-party apps made available through its app store limit collection of user information to what is directly relevant and necessary to accomplish the purpose of the app?
		P3(a).6	(For personal digital assistant ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party skills made available through its skill store disclose what user information the skills collects ?
		P3(a).7	(For personal digital assistant ecosystems): Does the company clearly disclose that it evaluates whether third-party skills made available through its skill store limit collection of user information to what is directly relevant and necessary to accomplish the purpose of the skill?

		P3(b)	Inference of user information: The company should clearly disclose what user information it infers and how.
		P3(b).1	Does the company clearly disclose all the types of user information it infers on the basis of collected user information ?
		P3(b).2	For each type of user information the company infers , does the company clearly disclose how it infers that user information ?
		P3(b).3	Does the company clearly disclose that it limits inference of user information to what is directly relevant and necessary to accomplish the purpose of its service?
P4	Sharing of user information The company should clearly disclose what user information it shares and with whom.	P4	Sharing of user information The company should clearly disclose what user information it shares and with whom.
P4.1	For each type of user information the company collects, does the company clearly disclose whether it shares that user information?	P4.1	For each type of user information the company collects, does the company clearly disclose whether it shares that user information?
P4.2	For each type of user information the company shares, does the company clearly disclose the types of third parties with which it shares that user information?	P4.2	For each type of user information the company shares , does the company clearly disclose the types of third parties with which it shares that user information?

P4.3	Does the company clearly disclose that it may share user information with government(s) or legal authorities?	P4.3	Does the company clearly disclose that it may share user information with government(s) or legal authorities?
P4.4	For each type of user information the company shares, does the company clearly disclose the names of all third parties with which it shares user information.	P4.4	For each type of user information the company shares , does the company clearly disclose the names of all third parties with which it shares user information?
P4.5	(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose what user information the apps share?	P4.5	(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third party apps made available through its app store disclose what user information the apps share ?
P4.6	(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose the types of third parties with whom they share user information?	P4.6	(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third party apps made available through its app store disclose the types of third parties with whom they share user information ?
		P4.7	(For personal digital assistant ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third party skills made available through its skill store disclose what user information the skills share ?
		P4.8	(For personal digital assistant ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third party skills made available through its skill store disclose the types of third parties with whom they share user information ?

P5	Purpose for collecting and sharing user information The company should clearly disclose why it collects and shares user information .	P5	Purpose for collecting, inferring, and sharing user information The company should clearly disclose why it collects , infers , and shares user information .
P5.1	For each type of user information the company collects, does the company clearly disclose its purpose for collection?	P5.1	For each type of user information the company collects , does the company clearly disclose its purpose for collection ?
		P5.2	For each type of user information the company infers , does the company clearly disclose its purpose for the inference ?
P5.2	Does the company clearly disclose whether it combines user information from various company services and if so, why?	P5.3	Does the company clearly disclose whether it combines user information from various company services and if so, why?
P5.3	For each type of user information the company shares, does the company clearly disclose its purpose for sharing?	P5.4	For each type of user information the company shares , does the company clearly disclose its purpose for sharing ?
P5.4	For each type of user information the company shares, does the company clearly disclose its purpose for sharing?	P5.5	Does the company clearly disclose that it limits its use of user information to the purpose for which it was collected or inferred ?
P6	Retention of user information: The company should clearly disclose how long it retains user information .	P6	Retention of user information: The company should clearly disclose how long it retains user information .
P6.1	For each type of user information the company collects, does the company clearly disclose how long it retains that user information?	P6.1	For each type of user information the company collects, does the company clearly disclose how long it retains that user information?

P6.2	Does the company clearly disclose what de-identified user information it retains?	P6.2	Does the company clearly disclose what de-identified user information it retains?
P6.3	Does the company clearly disclose the process for de-identifying user information ?	P6.3	Does the company clearly disclose the process for de-identifying user information ?
P6.4	Does the company clearly disclose that it deletes all user information after users terminate their account?	P6.4	Does the company clearly disclose that it deletes all user information after users terminate their account?
P6.5	Does the company clearly disclose the time frame in which it will delete user information after users terminate their account?	P6.5	Does the company clearly disclose the time frame in which it will delete user information after users terminate their account?
P6.6	(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose how long they retain user information?	P6.6	(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose how long they retain user information?
P6.7	(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store state that all user information is deleted when users terminate their accounts or delete the app?	P6.7	(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store state that all user information is deleted when users terminate their accounts or delete the app?
		P6.8	(For personal digital assistant ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party skills made available through its skill store disclose how long they retain user information ?
		P6.9	(For personal digital assistant ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party skills made available through its skill store state that all user information is deleted when users terminate their accounts or delete the skill ?

P7	Users' control over their own user information: The company should clearly disclose to users what options they have to control the company's collection, retention , and use of their user information.	P7	Users' control over their own user information: The company should clearly disclose to users what options they have to control the company's collection, inference, retention and use of their user information .
P7.1	For each type of user information the company collects, does the company clearly disclose whether users can control the company's collection of this user information?	P7.1	For each type of user information the company collects , does the company clearly disclose whether users can control the company's collection of this user information ?
P7.2	For each type of user information the company collects, does the company clearly disclose whether users can delete this user information?	P7.2	For each type of user information the company collects , does the company clearly disclose whether users can delete this user information ?
		P7.3	For each type of user information the company infers on the basis of collected information , does the company clearly disclose whether users can control if the company can attempt to infer this user information ?
		P7.4	For each type of user information the company infers on the basis of collected information , does the company clearly disclose whether users can delete this user information ?
P7.3	Does the company clearly disclose that it provides users with options to control how their user information is used for targeted advertising?	P7.5	Does the company clearly disclose that it provides users with options to control how their user information is used for targeted advertising ?
P7.4	Does the company clearly disclose that targeted advertising is off by default?	P7.6	Does the company clearly disclose whether targeted advertising is on or off by default?

		P7.6	Does the company clearly disclose that users can <i>opt in</i> to being served with targeted advertising ?
		P7.7	Does the company clearly disclose that it provides users with options to control how their user information is used for the development of algorithmic systems ?
		P7.8	Does the company clearly disclose whether it uses user information to develop algorithmic systems by default, or not?
P7.5	(For mobile ecosystems): Does the company clearly disclose that it provides users with options to control the device's geolocation functions?	P7.9	(For mobile ecosystems and personal digital assistant ecosystems): Does the company clearly disclose that it provides users with options to control the device's geolocation functions?
P8	Users' access to their own user information Companies should allow users to obtain all of their user information the company holds.	P8	Users' access to their own user information Companies should allow users to obtain all of their user information the company holds.
P8.1	Does the company clearly disclose that users can obtain a copy of their user information ?	P8.1	Does the company clearly disclose that users can obtain a copy of their user information ?
P8.2	Does the company clearly disclose what user information users can obtain?	P8.2	Does the company clearly disclose what user information users can obtain?
P8.3	Does the company clearly disclose that users can obtain their user information in a structured data format?	P8.3	Does the company clearly disclose that users can obtain their user information in a structured data format?

P8.4	Does the company clearly disclose that users can obtain all public-facing and private user information a company holds about them?	P8.4	Does the company clearly disclose that users can obtain all public-facing and private user information a company holds about them?
		P8.5	Does the company clearly disclose that users can obtain all the information that a company has inferred about them?
P8.5	(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose that users can obtain all of the user information about them the app holds?	P8.6	(For mobile ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party apps made available through its app store disclose that users can obtain all of the user information about them the app holds?
		P8.7	(For personal digital assistant ecosystems): Does the company clearly disclose that it evaluates whether the privacy policies of third-party skills made available through its skill store state that all user information is deleted when users terminate their accounts or delete the skill ?
P9	Collection of user information from third parties (internet and mobile ecosystem companies): The company should clearly disclose its practices with regard to user information it collects from third-party websites or apps through technical means .	P9	Collection of user information from third parties (internet and mobile ecosystem companies): The company should clearly disclose its practices with regard to user information it collects from third-party websites or apps through technical means , as well as user information it collects through non-technical means .
P9.1	Does the company clearly disclose what user information it collects from third-party websites through technical means?	P9.1	(For digital platforms) Does the company clearly disclose what user information it collects from third-party websites through technical means?

P9.2	Does the company clearly explain how it collects user information from third parties through technical means?	P9.2	(For digital platforms) Does the company clearly explain how it collects user information from third parties through technical means?
P9.3	Does the company clearly disclose its purpose for collecting user information from third parties through technical means?	P9.3	(For digital platforms) Does the company clearly disclose its purpose for collecting user information from third parties through technical means?
P9.4	Does the company clearly disclose how long it retains the user information it collects from third parties through technical means?	P9.4	(For digital platforms) Does the company clearly disclose how long it retains the user information it collects from third parties through technical means?
P9.5	Does the company clearly disclose that it respects user-generated signals to opt-out of data collection?	P9.5	(For digital platforms) Does the company clearly disclose that it respects user-generated signals to opt-out of data collection?
		P9.6	Does the company clearly disclose what user information it collects from third-parties through non-technical means?
		P9.7	Does the company clearly explain how it collects user information from third parties through non-technical means?
		P9.8	Does the company clearly disclose its purpose for collecting user information from third parties through non-technical means?

		P9.9	Does the company clearly disclose how long it retains the user information it collects from third parties through non-technical means?
P10	Process for responding to third-party requests for user information The company should clearly disclose its process for responding to requests from governments and other third parties for user information.	P10(a)	Process for responding to government third-party demands requests for user information The company should clearly disclose its process for responding to requests from governments demands and other third parties for user information.
P10.1	Does the company clearly disclose its process for responding to non-judicial government requests ?	P10(a).1	Does the company clearly disclose its process for responding to non-judicial government demands requests ?
P10.2	Does the company clearly disclose its process for responding to court orders ?	P10(a).2	Does the company clearly disclose its process for responding to court orders ?
P10.3	Does the company clearly disclose its process for responding to government requests from foreign jurisdictions?	P10(a).3	Does the company clearly disclose its process for responding to government demands requests from foreign jurisdictions?
		P10(a).4	Does the company clearly disclose its process for responding to requests made by private parties?
P10.5	Do the company's explanations clearly disclose the legal basis under which it may comply with government requests ?	P10(a).4	Do the company's explanations clearly disclose the legal basis under which it may comply with government demands requests ?

		P10(a).6	Do the company's explanations clearly disclose the basis under which it may comply with requests from private parties?
P10.7	Does the company clearly disclose that it carries out due diligence on government requests before deciding how to respond?	P10(a).5	Does the company clearly disclose that it carries out due diligence on government demands requests before deciding how to respond?
		P10.8	Does the company clearly disclose that it carries out due diligence on private requests before deciding how to respond?
P10.9	Does the company commit to push back on inappropriate or overbroad government requests ?	P10.5	Does the company commit to push back on inappropriate or overbroad government demands requests ?
		P10.10	Does the company commit to push back on inappropriate or overbroad private requests?
P10.11	Does the company provide clear guidance or examples of implementation of its process for government requests ?	P10.7	Does the company provide clear guidance or examples of implementation of its process for government demands requests ?
		P10.12	Does the company provide clear guidance or examples of implementation of its process for private requests?
		P10(b)	Process for responding to private requests for user information: The company should clearly disclose its process for responding to requests for user information that come through private processes ?

P10.4	Does the company clearly disclose its process for responding to requests made by private parties ?	P10(b).1	Does the company clearly disclose its process for responding to private requests to remove, filter, or restrict content or accounts made through private processes ?
P10.6	Do the company's explanations clearly disclose the basis under which it may comply with requests from private parties ?	P10(b).2	Do the company's explanations clearly disclose the basis under which it may comply with private requests made through private process ?
P10.8	Does the company clearly disclose that it carries out due diligence on private requests before deciding how to respond?	P10(b).3	Does the company clearly disclose that it carries out due diligence on private requests made through private processes before deciding how to respond?
P10.10	Does the company commit to push back on inappropriate or overbroad private requests ?	P10(b).4	Does the company commit to push back on inappropriate or overbroad private requests made through private processes ?
P10.12	Does the company provide clear guidance or examples of implementation of its process for private requests ?	P10(b).5	Does the company provide clear guidance or examples of implementation of its process of responding to private requests made through private processes ?
P11	Data about third-party requests for user information The company should regularly publish data about government and other third-party requests for user information .	P11(a)	Data about government third-party requests for user information The company should regularly publish data about government demands and other third-party requests for user information .

P11.1	Does the company list the number of requests it receives by country?	P11(a).1	Does the company list the number of government demands requests it receives by country?
P11.2	Does the company list the number of requests it receives for stored user information and for real-time communications access ?	P11(a).2	Does the company list the number of government demands requests it receives for stored user information and for real-time communications access ?
P11.3	Does the company list the number of accounts affected?	P11(a).3	Does the company list the number of accounts affected?
P11.4	Does the company list whether a demand sought communications content or non-content or both?	P11(a).4	Does the company list whether a demand sought communications content or non-content or both?
P11.5	Does the company identify the specific legal authority or type of legal process through which law enforcement and national security demands are made?	P11(a).5	Does the company identify the specific legal authority or type of legal process through which law enforcement and national security demands are made?
P11.6	Does the company include requests that come from court orders ?	P11(a).6	Does the company include government demands requests that come from court orders ?
		P11(a).7	Does the company list the number of requests it receives from private parties?
P11.8	Does the company list the number of requests it complied with, broken down by category of demand?	P11(a).8	Does the company list the number of government demands requests it complied with, broken down by category of demand?

P11.9	Does the company list what types of government requests it is prohibited by law from disclosing?	P11(a).9	Does the company list what types of government demands requests it is prohibited by law from disclosing?
P11.10	Does the company report this data at least once per year?	P11(a).10	Does the company report this data at least once per year?
P11.11	Can the data reported by the company be exported as a structured data file?	P11.(a).11	Can the data reported by the company be exported as a structured data file?
		P11(b)	Data about private requests for user information The company should regularly publish data about requests for user information that come through private processes .
P11.7	Does the company list the number of requests it receives from private parties?	P11(b).1	Does the company list the number of requests it receives for user information from private parties that come through private processes ?
		P11(b).2	Does the company list the number of requests for user information that come through private processes with which it complied?
		P11(b).3	Does the company report this data at least once per year?
		P11(b).4	Can the data reported by the company be exported as a structured data file?

P12	User notification about third-party requests for user information The company should notify users to the extent legally possible when their user information has been requested by governments and other third parties.	P12	User notification about third-party requests for user information The company should notify users to the extent legally possible when their user information has been requested by governments and other third parties .
P12.1	Does the company clearly disclose that it notifies users when government entities (including courts or other judicial bodies) request their user information ?	P12.1	Does the company clearly disclose that it notifies users when government entities (including courts or other judicial bodies) request their user information ?
P12.2	Does the company clearly disclose that it notifies users when private parties request their user information ?	P12.2	Does the company clearly disclose that it notifies users when they receive private parties requests their user information through private processes ?
P12.3	Does the company clearly disclose situations when it might not notify users, including a description of the types of government requests it is prohibited by law from disclosing to users?	P12.3	Does the company clearly disclose situations when it might not notify users, including a description of the types of government requests it is prohibited by law from disclosing to users?
P13.	Security oversight The company should clearly disclose information about its institutional processes to ensure the security of its products and services.	P13.	Security oversight The company should clearly disclose information about its institutional processes to ensure the security of its products and services.
P13.1	Does the company clearly disclose that it has systems in place to limit and monitor employee access to user information?	P13.1	Does the company clearly disclose that it has systems in place to limit and monitor employee access to user information ?
P13.2	Does the company clearly disclose that it has a security team that conducts security audits on the company's products and services?	P13.2	Does the company clearly disclose that it has a security team that conducts security audits on the company's products and services?

P13.3	Does the company clearly disclose that it commissions third-party security audits on its products and services?	P13.3	Does the company clearly disclose that it commissions third-party security audits on its products and services?
P14	Addressing security vulnerabilities The company should address security vulnerabilities when they are discovered.	P14	Addressing security vulnerabilities The company should address security vulnerabilities when they are discovered.
P14.1	Does the company clearly disclose that it has a mechanism through which security researchers can submit vulnerabilities they discover?	P14.1	Does the company clearly disclose that it has a mechanism through which security researchers can submit vulnerabilities they discover?
P14.2	Does the company clearly disclose the timeframe in which it will review reports of vulnerabilities ?	P14.2	Does the company clearly disclose the timeframe in which it will review reports of vulnerabilities ?
P14.3	Does the company commit not to pursue legal action against researchers who report vulnerabilities within the terms of the company's reporting mechanism?	P14.3	Does the company commit not to pursue legal action against researchers who report vulnerabilities within the terms of the company's reporting mechanism?
P14.4	(For mobile ecosystems) Does the company clearly disclose that software updates , security patches , add-ons, or extensions are downloaded over an encrypted channel?	P14.4	(For mobile ecosystems and personal digital assistant ecosystems) Does the company clearly disclose that software updates , security patches , add-ons, or extensions are downloaded over an encrypted channel?
P14.5	(For mobile ecosystems and telecommunications companies) Does the company clearly disclose what, if any, modifications it has made to a mobile operating system ?	P14.5	(For mobile ecosystems and telecommunications companies) Does the company clearly disclose what, if any, modifications it has made to a mobile operating system ?
P14.6	(For mobile ecosystems and telecommunications companies) Does the company clearly disclose what,	P14.6	(For mobile ecosystems, personal digital assistant ecosystems , and telecommunications companies)

	if any, effect such modifications have on the company's ability to send security updates to users?		Does the company clearly disclose what, if any, effect such modifications have on the company's ability to send security updates to users?
P14.7	(For mobile ecosystems) Does the company clearly disclose the date through which it will continue to provide security updates for the device/OS ?	P14.7	(For mobile ecosystems and personal digital assistant ecosystems) Does the company clearly disclose the date through which it will continue to provide security updates for the device/OS ?
P14.8	(For mobile ecosystems) Does the company commit to provide security updates for the operating system and other critical software for a minimum of five years after release?	P14.10	(For mobile ecosystems and personal digital assistant ecosystems) Does the company commit to provide security updates for the operating system and other critical software for a minimum of five years after release?
P14.9	(For mobile ecosystems and telecommunications companies) If the company uses an operating system adapted from an existing system, does the company commit to provide security patches within one month of a vulnerability being announced to the public?	P14.11	(For mobile ecosystems, personal digital assistant ecosystems , and telecommunications companies) If the company uses an operating system adapted from an existing system, does the company commit to provide security patches within one month of a vulnerability being announced to the public?
		P14.12	(For personal digital assistant ecosystems): Does the company clearly disclose what, if any, modifications it has made to a personal digital assistant operating system ?
		P14.13	(For personal digital assistant ecosystems): Does the company clearly disclose what, if any, effect such modifications have on the company's ability to send security updates to users ?

P15	Data breaches The company should publicly disclose information about its processes for responding to data breaches .	P15	P15. Data breaches The company should publicly disclose information about its processes for responding to data breaches .
P15.1	Does the company clearly disclose that it will notify the relevant authorities without undue delay when a data breach occurs?	P15.1	Does the company clearly disclose that it will notify the relevant authorities without undue delay when a data breach occurs?
P15.2	Does the company clearly disclose its process for notifying data subjects who might be affected by a data breach ?	P15.2	Does the company clearly disclose its process for notifying data subjects who might be affected by a data breach ?
P15.3	Does the company clearly disclose what kinds of steps it will take to address the impact of a data breach on its users?	P15.3	Does the company clearly disclose what kinds of steps it will take to address the impact of a data breach on its users?
P16	Encryption of user communication and private content (internet and mobile ecosystem companies) The company should encrypt user communication and private content so users can control who has access to it.	P16	P16. Encryption of user communication and private content (digital platforms-internet and mobile ecosystem-companies) The company should encrypt user communication and private content so users can control who has access to it.
P16.1	Does the company clearly disclose that the transmission of user communications is encrypted by default?	P16.1	Does the company clearly disclose that the transmission of user communications is encrypted by default?

P16.2	Does the company clearly disclose that transmissions of user communications are encrypted using unique keys?	P16.2	Does the company clearly disclose that transmissions of user communications are encrypted using unique keys?
P16.3	Does the company clearly disclose that users can secure their private content using end-to-end encryption , or full-disk encryption (where applicable)?	P16.3	Does the company clearly disclose that users can secure their private content using end-to-end encryption , or full-disk encryption (where applicable)?
P16.4	Does the company clearly disclose that end-to-end encryption , or full-disk encryption , is enabled by default?	P16.4	Does the company clearly disclose that end-to-end encryption , or full-disk encryption , is enabled by default?
P17.	Account Security (internet and mobile ecosystem companies) The company should help users keep their accounts secure.	P17.	P17. Account Security (digital platforms-internet and mobile ecosystem companies) The company should help users keep their accounts secure.
P17.1	Does the company clearly disclose that it deploys advanced authentication methods to prevent fraudulent access?	P17.1	Does the company clearly disclose that it deploys advanced authentication methods to prevent fraudulent access?
P17.2	Does the company clearly disclose that users can view their recent account activity?	P17.2	Does the company clearly disclose that users can view their recent account activity?
P17.3	Does the company clearly disclose that it notifies users about unusual account activity and possible unauthorized access to their accounts?	P17.3	Does the company clearly disclose that it notifies users about unusual account activity and possible unauthorized access to their accounts?
P18.	Inform and educate users about potential risks	P18.	Inform and educate users about potential risks

	The company should publish information to help users defend themselves against cyber risks .		The company should publish information to help users defend themselves against cyber risks .
P18.1	Does the company publish practical materials that educate users on how to protect themselves from cyber risks relevant to their products or services?	P18.1	Does the company publish practical materials that educate users on how to protect themselves from cyber risks relevant to their products or services?
		P19.	P19. User access to advertising targeting metadata The company should clearly disclose how users can access key information about the targeted advertising that they see.
		P19.1	Does the company clearly disclose how users can access the list of advertising audience categories to which the company has assigned them?
		P19.2	Does the company clearly disclose how users can access the list of advertising audience categories to which each piece of advertising content they see while using the product or service was targeted ?
		P19.3	Does the company clearly disclose how users can access the list of advertisers who have attempted to influence them through the company's on-platform targeted advertising technologies?
		P19.4	Does the company clearly disclose how users can access the list of advertising audience categories to which each piece of advertising content they see off-platform was targeted through the company's advertising network ?

			P19.5	Does the company clearly disclose how users can access the list of advertisers who have attempted to influence them through the company's off-platform advertising network ?
--	--	--	-------	--