Submission # 77

Name: Sunny Kang

Organization: Electronic Privacy Information Center

How would you define the stakeholder community or communities to which you belong?

Civil society

Are there any suggestions that you wish to make in respect of the proposed themes, questions and indicators which are included in the framework as it stands?

I. Include Algorithmic Transparency as a Cross-Cutting Indicator
EPIC supports the recognition of algorithmic transparency as a fundamental human right.10 EPIC campaigned for transparency and accountability in government and commercial uses of secret algorithms for many years.11 Our push for algorithmic transparency has addressed secret government profiling systems in the United States and around the world.
We must know the basis of decisions, whether right or wrong. But as decisions are automated, and organizations increasingly delegate decision-making to techniques they do not fully understand, processes become more opaque and less accountable.
If, for example, a government agency considers a factor such as race, gender, or religion to produce an adverse decision, then the decision-making process should be subject to scrutiny and the relevant factors identified. It is therefore imperative that algorithmic processes be open, provable, and accountable.
EPIC advocates for the inclusion of algorithmic transparency as a cross-cutting indicator to inform each assessment of the themes in the ROAM framework. Algorithmic transparency is integral to the nexus of accountability and Internet Universality, and we believe that it is a critical indicator of rights, openness, access, and multistakeholder participation.
1. The Use of Secret Algorithms is Increasing
The proliferation of secret algorithms for governmental and commercial use threatens the exercise of rights that underpin individual autonomy and liberty. Algorithms are often used to make adverse decisions about people. Algorithms deny people educational opportunities, employment, housing, insurance, and credit.12 Many of these decisions are entirely opaque, leaving individuals to wonder whether the decisions were accurate, fair, or even about them. Therefore, algorithmic transparency is critical to ensuring accountability in the input of an automated decision-making process, as well as the rationale for a specific decision impacting the subject's rights and opportunities. It is timely to address this now, as reliance on secret algorithms is rapidly increasing on a global scale. For example:
■ In the United States, secret algorithms are deployed in the criminal justice system to assess forensic evidence, determine sentences, and even to decide guilt or innocence.13 Several states use proprietary commercial systems, not subject to open government laws, to determine guilt or innocence. The Model Penal Code recommends the implementation of recidivism-based actuarial instruments in sentencing guidelines.14 But these systems, which defendants may have no opportunity to challenge, can be racially biased,

unaccountable, and unreliable for forecasting violent crime.15

■ Algorithms are used for social control. The Chinese government is deploying a "social credit" system that assigns to each person a government-determined favorability rating. "Infractions such as fare cheating, jaywalking, and violating family-planning rules" would affect a person's rating.16 Low ratings are also assigned to those who frequent disfavored web sites or socialize with others who have low ratings. Citizens with low ratings will have trouble getting loans or government services. Citizens with high ratings, assigned by the government, receive preferential treatment across a wide range of programs and activities.

■ In the United States, Customs and Border Protection has used secret analytic tools to assign "risk assessments" to U.S. travelers.17 These risk assessments, assigned by the U.S. government to U.S. citizens, raise fundamental questions about government accountability, due process, and fairness.

A German company called Kreditech deploys a proprietary credit-scoring algorithm to process up to 20,000 data points on the loan applicant's social media networks, e-commerce behavior, and web analytics.18 Information about the applicant's social media friends are collected to assess the applicant's "decision-making quality" and creditworthiness. Kreditech's Chief Financial Officer, Rene Griemens, told the Financial Times that being connected to someone who has already satisfied a loan with the company is "usually a good indicator."19

■ More loan companies are factoring in social media activity to determine whether to make a credit offer. In India and Russia, Fair Isaac Corp ("FICO") is partnering with startups like Lenddo to process large quantities of data from the applicant's mobile phone to conduct predictive credit-risk assessments.20 Lenddo collects longitudinal location data to verify the applicant's residence and work address, then analyzes the applicant's interpersonal communications and associations on social media to produce a credit score.21 Secret profiling based on personal web activity infringes the fundamental rights to privacy and access to information, but it is perilously becoming normalized and rebranded as "online verification methods."

■ "Social scoring" is a growing focus of cultural dystopias.22 The recognition that the technique could become widespread is self-evident.23

EPIC believes that the ROAM framework should promote algorithmic transparency as a central goal to Internet Universality, and establish a mandate for multistakeholders to address the alarming inequities of automated profiling.

We encourage the initiatives of computer science organizations, such as the Association for Computing Machinery ("ACM")24 and IEEE25, in producing quantitative research on algorithmic discrimination to inform regulators. We also applaud the efforts of government bodies, such as the New York City Council26 and the UK Parliament's Science and Technology Committee,27 on their inquiries into transparency in algorithmic decision-making.

2. Fundamental Rights and Institutions at Stake

Algorithmic transparency is foundational to the protection of other fundamental human rights: the right to privacy, freedom of expression, and the right to access information from an accountable source. These rights are indispensable to the integrity and quality of democratic governance.

A. Right to Privacy

EPIC remains concerned about the lack of international legal and policy frameworks that ensure a privacy right to be aware of the application of algorithms to one's personal data, and the right to contest both the logic and outcome of a specific automated decision. Right to be informed about the existence of automatic decision-making must be accompanied by the right to an explanation of the algorithmic consequences—to protect privacy rights with complete

accountability and heightened data protection standards.

B. Right to Free Expression

Free speech rights are also curtailed when platforms use secret algorithms to automatically filter online content. Without accountability and transparency for such mechanisms, the free exchange of ideas on the web would be severely obstructed by "privatized," extrajudicial censorship without due process. Algorithmic transparency on the filtering criteria is imperative to identify potential biases in the natural language processing system and its training corpus. Transparency safeguards the cultural diversity of the Internet by upholding the exercise of free expression, and ensures an open web where ideas can be exchanged without the domination of one particular viewpoint favored by an algorithm.

C. Right to Access Information

Algorithms that rank and index search results must also be scrutinized for distorting web users' access to information with limited transparency and accountability. Virtually every search engine, social media company, and web operator develops its own unique algorithm to curate content for individual users to control how information is fetched and displayed from search queries.28

There are many dangers with these information mediating techniques.

■ Filtering algorithms can prevent individuals from using the Internet to exchange information on topics that may be controversial or unpopular.

■ Content may be labelled and categorized according to a rating system designed by governments to enable censorship and block access to political opposition or specific keywords.

■ ISPs may block access to content on entire domains or selectively filter out web content available at any domain or page which contains a specific keyword or character string in the URL.

■ Self-rating schemes by private entities will turn the Internet into a homogenized medium dominated by commercial speakers.

■ Self-rating schemes will embolden and encourage government regulation on access to information on the Internet.

■ The majority of users are unaware of how algorithmic filtering restricts their access to information and do not have an option to disable filters.

D. Integrity of the Democratic Process

EPIC supports algorithmic transparency requirements for targeted political advertisements in online platforms.29 Algorithms now enable targeted ads with unprecedented granularity. This technology surpasses the reach of traditional media and necessitates greater disclosure requirements from online advertisers, as algorithms can be misused for disinformation campaigns that propagate divisive messages to demographic targets and disrupt democratic elections.

Social media's vulnerability to illicit interference on democratic discourse is exacerbated by the lack of transparency on who paid for a targeted communication directed to a specific user or group. The current system is imbalanced: voters know who paid for a mass advertisement that appears on television or in a newspaper but are left in the dark about the source, purpose, and scope of a targeted political advertisement that infiltrates their digital media platforms. This information asymmetry destabilizes the election process by allowing companies like Facebook, Twitter, and Google to circumvent the disclosure rules that govern traditional media.

EPIC believes that algorithmic transparency is necessary whenever there is processing of personal data that generates targeted campaign advertising. Companies are hiding behind privacy claims to shield their business practices from scrutiny.30 A bright-line can be drawn between paid commercial advertising and user-generated content in order to protect free speech and privacy rights.

Algorithmic transparency requirements should obligate full disclosures on how an advertiser used its tools to create a target audience for that advertisement, including what data it collected about the user that caused the user to be placed within that target audience. These disclosures would establish accountability for the use of online political advertising and help

users evaluate the arguments to which they are being subjected.

3. International Guidance on Algorithmic Transparency is Imperative

The European Union has recognized that secret algorithms cause substantial harm. Article 15 of the EU Data Protection Directive, which followed from the U.S. Privacy Act of 1974, provides that individuals have a right to access "the logic of the processing" concerning their personal information.31 The provision of Article 15 in the EU Data Protection Directive ("Directive") has been carried forward in Article 13 of the recently adopted General Data Protection Regulation ("GDPR").

EPIC believes that the UNESCO Internet Universality framework presents a timely opportunity to address and clarify these issues. We suggest the following themes, questions, and indicators to evaluate the impact of algorithmic transparency on fundamental rights, the openness and accessibility of the Internet, and multistakeholder goals.

II. Thematically Assess Algorithmic Transparency on Awareness, Accessibility, and Accountability

The continued deployment of AI-based systems raises profound issues for all countries. Secret algorithms are trending because institutions evade rigorous testing of their computational models by hiding behind technical excuses (arguing that algorithmic transparency is impossible due to the complexity and fluidity of modern processes), economic justifications (the cost of preparing an explanation that can be rationalized by a human is prohibitive), and legal interests (opacity is necessary to protect intellectual property rights and trade secrets). However, computer scientists have made clear the need to explore potential biases and errors in the "black box" of predictive algorithms and analytics.32 As Professor Frank Pasquale has said:

> Black box services are often wondrous to behold, but our black box society has become dangerously unstable, unfair, and unproductive. Neither New York quants nor California engineers can deliver a sound economy or a secure society. Those are the tasks of a citizenry, which can perform its job only as well as it understands the stakes.33

The goal of the "Awareness" theme is to assess whether individual rights are protected against algorithmic profiling and discrimination through the right to examine the design, implementation, and consequences of automated processing. This indicator provides checkpoints for transparency and accuracy at each processing stage to improve data governance, data quality, and the opportunity to correct hidden bias.

The "Accessibility" theme assesses the fairness of processing through the right to explanation, particularly on the existence of actionable mechanisms for individuals to examine the algorithm's "logic process" and the factors contributing to an automated decision. This additional safeguard is critical to the protection of individual rights, because even accurate input can be distorted by a particular analytic model to extrapolate biased inferences that result in profiling and algorithmic discrimination.

Finally, the "Accountability" theme assesses the individual's rights to invoke remedies and obtain redress from adverse decisions made by algorithms. The touchstone of algorithmic transparency is the responsibility of institutions to justify the provability of their own analytic systems and to address potential and actualized harms. Therefore, this indicator establishes baselines for legal and regulatory measures to contest automated decisions, and enforcement mechanisms to end opaque practices that threaten fundamental rights.

1. Awareness

1.A: Are there legal or regulatory safeguards to be notified as a subject of automated processing?

Indicators:

■ Laws or regulations for data controllers to notify individuals when their personal data is being processed for automated decision-making.

■ Further notification requirements on the purpose and extent of the processing, and an explanation of the envisaged consequences of the automated decision.

1.B: Are effective arrangements in place to correct inaccurate, incomplete, or outdated data about oneself in automated processing?

Indicators:

■ Decision-making algorithms should identify itself to the subject and explain the personal data collected for processing and how they will be weighed to make determinations.

■ Existence of legal standards on data provenance, and the comprehensiveness of those laws.
■ Individuals have the ability to examine the lawfulness or validity of processing, and have recourse to invoke legal remedies.

Public record of validation and testing of computational models used for input and output.
2. Accessibility
2.A: Do data controllers have a legal or regulatory obligation to explain the algorithmic procedures (input) as well as the reason behind the decision (output)?
Indicators:
■ An independent legal or regulatory authority to implement algorithmic transparency requirements on stakeholders of analytic systems.
■ Clear legal and regulatory standards on the extent of disclosure required for the “logic of the process” and what qualifies as a “meaningful explanation” of decisions.
■ Consumer perception of regulatory performance on enforcing transparency requirements.

2.B: Are there legal standards for data governance that compel effective right of access?
Indicators:
■ Regulation of internal record keeping to ensure that analytics companies can process subject access requests on automated processing. I.e. the ability to query their data to find all the information they have on an individual.
■ Industry practice of enabling users to securely access their data to identify its source and purpose through a web portal.
■ Regulation to limit secondary uses of data collected for automated processing, and enforcement action against companies that do not maintain records of the specific purposes of data processing or exceed their stated purpose.
3. Accountability
3.A: Are effective arrangements in place to contest a specific automated decision?
Indicators:
■ No unreasonable evidentiary burden on “injury” to bring a claim.
■ The right to contest an automated decision is actionable even if the algorithm was applied to a group rather than an individual.

The rights to explanation and redress are actionable even if the algorithm merely “factored into” the automated decision-making without actually making the decision. The fact that a decision was not “solely” based on the algorithm does not preclude a claim.
■ Engagement of third party auditors where harm is suspected from automated processes.
■ Implementation of machine learning to differentiate correlation and causation to improve the accuracy of automated decisions.

3.B: Is there a legal right to opt-out of automated processing?
Indicators:
■ Legal protection against automated decision-making by default, where the data processor must prove an exemption to the prohibition through contract or explicit consent.
■ Whenever practicable, individuals have the option to opt-out to avoid foreseeable injury.
■ If transparency is achievable with an alternative system based on objective and provable metrics, then proprietary algorithms are not deployed.

Are there any suggestions that you wish to make in respect of the proposed themes, questions and indicators which are included in the framework as it stands?

1. Rule of Law
■ Many indicators conflate two different factors: the existence of legal frameworks, and

effective implementation. Each aspect should be measured separately, not in a single indicator.
■ Indicators should individually assess the existence of a legal framework and the adequacy of those laws in protecting human rights. The substantive quality of laws should be examined by the comprehensiveness of the statute and whether the public policy aims are consistent with international rights agreements.
■ Indicators should then query the procedural quality of laws by assessing the safeguards for due process, existence of independent enforcement agencies, and whether those agencies have sufficient resources and funding to enforce promptly, effectively, and authoritatively to set precedent amongst Internet stakeholders.
■ In particular, institutional adherence to the rule of law is indicative of an effective and fair legal framework to address Internet Universality issues. EPIC suggests incorporating rule of law principles into the assessment of the ROAM framework, to ensure that the UNESCO indicators are substantiated by access to justice, an independent judiciary, an open and accountable government, and egalitarian protections for fundamental rights.

2. Reporting Bias
■ Many indicators refer to 'credible sources'. Reporting bias is a persistent problem with institutionally driven indicators. This avoids scientific and quantitative rigor and weakens the capacity for evidence-based policy.

■ Each indicator should include the specification of the statistical model and a well-documented (replicable) reporting bias-free data collection process. When data is to be

collected from expert opinion or specialized organizations, source of funding and conflict of interest should be explicitly described for each indicator for each one of the sources, including why that source is considered credible, and how the data was computed to produce the indicator.
■ When raw data is processed (i.e. extracting claims from texts) the code books and the description of any processing should be included as well.

II. Multistakeholder Indicator
1. Market Structure and Incentives
■ Commercial stakeholders are often driven by business incentives, and the current ROAM framework does not address the pitfalls of co-regulatory and industry-led standard setting on privacy and free expression.
■ No indicator is offered to estimate the market effects of digital public policy, and how this may impact multistakeholder participation. It is necessary to measure the economic tradeoffs of investing in certain technologies over another, and engage in interdisciplinary (economic, legal, and behavioral) analysis on raising enforcement penalties against violators of digital rights.
For example, companies may not be economically incentivized to minimize data collection and implement Privacy Enhancing Techniques (“PETs”) over Privacy Invasive Techniques (“PITs”) without legal pressure through soft and hard law.
■ Another example, is that intermediary platforms are risk-averse towards user communications and will advocate for safe harbor laws that encourage extrajudicial censorship by over-removal.
■ Therefore, indicators should address market structures, such as information asymmetry, monopolies, and competition, that fragment multistakeholder agendas.
■ Stakeholder participation in internet governance should be measured by practical outcomes in legislative reform and policy progress, rather than mere participation in forums such as IGF and ICANN.

What sources and means of verification would you recommend, from your experience, in relation to any of the questions and indicators that have been proposed?

I. Evidence-Based Policymaking

1. Privacy Concerns in Open Data

EPIC has a particular interest in safeguarding personal privacy and preventing harmful data practices. We encourage the broader use of statistical data for evidence-based policymaking, but also emphasize the importance of quantitative methodologies that are transparent, provable, and protective of individual privacy rights. 34

Evidence-based policy requires (1) an independent agency to facilitate access to data and oversee the use of multiple data sources, and (2) a legal mandate to use the strongest privacy protocols on personally identifiable information ("PII") while permitting statistical use.35

■ Although increased use of administrative and survey data has the potential to improve informed policymaking, there are real risks in combining this data and making it more easily available. Data that is improperly protected can be used by the government and in the private sector for profiling, tracking, and discrimination. The potential uses of personal information to make automated decisions and segregate individuals based on secret, imprecise and oftentimes impermissible factors present clear risks to fairness and due process.36

■ The ROAM framework should qualify the principle of "Open Data" with legal safeguards to ensure that government agencies collecting and amassing PII are under obligation to protect individual privacy. Privacy must be an integral component of any effort to streamline access to administrative and survey data.

■ These safeguards should include strict government adherence to Fair Information Practices ("FIPs"). A legal framework regulating the collection, maintenance, use, and dissemination of information by government agencies must be prerequisite to open data policies.

■ In particular, indicators should ensure that open data policies direct data clearing houses to minimize the collection of PII, secure the information collected, and prevent abusive uses of predictive analytics. Systems should also be in place to allow individuals to access and amend inaccurate records. Since the idea of a centralized repository is particularly worrisome, any clearinghouse should leave data with the custodial agencies.

■ Legal and technical frameworks must implement PETs in open data to minimize PII collection by design. This would encompass privacy-protective data analysis methods, cryptography, and differential privacy to prevent re-identification of multiple data points on an individual.

For further information on evidence-based policymaking and privacy, please consult the publications "Innovations in Federal Statistics: Combining Data Sources While Protecting Privacy"37 and "Federal Statistics, Multiple Data Sources, and Privacy Protection: Next Steps."38