



CCC

Computing Community Consortium
Catalyst

Response to RFI on Federal Priorities for Information Integrity Research and Development

May 13, 2022

Written by: Nadya Bliss (Arizona State University), David Danks (University of California, San Diego), Brian LaMacchia (Microsoft Research), Katie Siek (Indiana University, Bloomington) and Ufuk Topcu (University of Texas at Austin)

From the start, we would like to stress that there have been many efforts to qualify narratives and networks in this space, but relatively few that are identifying methods or solutions. A large amount of research is needed to address a complex set of challenges in the information integrity space. The Computing Community Consortium addressed a number of these points in a 2020 white paper "[An Agenda for Disinformation Research](#)". The paper describes a multi-disciplinary research agenda incorporating disinformation detection, education, measurements of impact, and a new common research infrastructure to combat disinformation and its effects upon the US and the world.

In this document we outline the specific challenges and research problems that we view as vital to mitigate the risks involved in mis/disinformation and work towards a more trustful information ecosystem.

1. Understanding the information ecosystem: There are many components, interactions, incentives, social, psychological, physiological, and technological aspects, and other considerations that can be used to effectively characterize the information ecosystem. What are the key research challenges in providing a common foundation for understanding information manipulation within this complex information ecosystem?

In order to establish a common foundation for understanding misinformation within the information ecosystem, we must address the following challenges:

- **Developing better, more relevant models of social and psychological phenomena** — sociotechnical behavioral models are often outdated and do not include new sociotechnical systems. This phenomenon ties into the fact that current models do not take into account the dynamic, continuously developing world that the information ecosystem is housed.
- **Creating frameworks for complex dynamics** — which involve the source of mis/dis-information, the medium in which they propagate, and the population they

target. These frameworks become even harder to create when the population that they target is the medium in which it propagates. To complicate things even further, the medium in which it propagates is affected by the technological platforms as well as the relationships between people in those platforms and outside.

- **Detecting sources of disinformation across scales** — the scale of the impact is very different from everything else we deal with. As a result, we need to find new methods of detecting sources of disinformation.
- **Developing mechanisms for countering mis/dis-information** — thinking about how to scale the pace of propagation to suppress mis/dis-information.
- **Metrics** — there has been a lot of appreciating the problem, but not enough of developing solutions and discussing what goes into determining if these solutions are successful. We not only need to discuss what constitutes success but ways to measure the impacts that mis/dis-information has on society.
- **Data infrastructure** — not only technical infrastructures and data sets, but also data infrastructure that acknowledges the context and socio-behavioral systems that impact these data systems.
- **Ethical research** — researchers must consider people's awareness of being included in studies and data sets and how this collection of data could adversely impact individuals going forward (e.g., someone being targeted by a disinformation campaign and then distributing the misinformation that is saved forever in a dataset). There have been studies that show people are not as aware as we think. We must also acknowledge that interventions prioritize a specific value set that may not translate across cultures, thus we should monitor and reflect on possible harms this may cause.

2. Preserving information integrity and mitigating the effects of information manipulation: Strategies for protecting information integrity must integrate the best technical, social, behavioral, cultural, and equitable approaches. These strategies should accomplish a range of objectives including to detect information manipulation, discern the influence mechanisms and the targets of the influence activities, mitigate information manipulation, assess how individuals and organizations are likely to respond, and build resiliency against information manipulation. What are the key gaps in knowledge or capabilities that research should focus on, in order to advance these objectives? What are the gaps in knowledge regarding the differential impact of information manipulation and mitigations on different demographic groups?

While disinformation is not new, confluence of technology and disinformation techniques (across media modalities - narrative, photo, video, etc.), creates an asymmetric vulnerability surface - it is significantly easier (cheaper, scalable) to create and propagate disinformation, than it is to counter it. Detecting and mitigating information manipulation at scale is a fundamentally interdisciplinary challenge.

Strategies for protecting information integrity must account for a wide variety of requirements. Some of these requirements may be in conflict with each other and will certainly evolve over time. There is a need for a framework that can distill and encode

these heterogeneous requirements and help identify the trade-offs between them in a way that can be understood by all stakeholders.

Research is needed to understand impacts of both disinformation and mitigation techniques. To do that effectively requires bringing together computer scientists, psychologists, and social scientists. Susceptibility to disinformation based on various characteristics also needs to be rigorously studied. Particularly, "psychological" isn't on this list, even though psychological knowledge (i.e., how does information manipulation impact cognition, particularly in ways that lead to problematic feedback loops?) is one of the big things that we don't really know and is an extremely important piece to this puzzle.

3. Information awareness and education: A key element of information integrity is to foster resilient and empowered individuals and institutions that can identify and abate manipulated information and create and utilize trustworthy information. What issues should research focus on to understand the barriers to greater public awareness of information manipulation? What challenges should research focus on to support the development of effective educational pathways?

An essential piece to overcoming the barriers that prevent public awareness of information manipulation is first understanding the impact that disinformation has on these communities. Currently, we don't fully understand the depth or the breadth dis/misinformation has on different communities. Are there actually different impacts based on demographics, or is it different impacts based on different features/properties (that happen to show up in different groups?). That is, could there be a "unified" model here? Citizens are confronted with a slew of information daily. There is no way for them to know what is true and what is not. After we understand the impact and the root of why audiences buy into dis/misinformation, we can start to reestablish trust with the community.

In a different vein, education/awareness might not be the right pathway here. There are lots of studies showing that people are still susceptible to mis/disinformation, even when they know that it is mis/disinformation. Take the example of vaccines. There was lots of fake information circulating the media and platforms about how dangerous the vaccines were, that the government was using vaccines to microchip citizens etc. People forgot about the vaccines they had already received and have no problem with. It is extremely hard to change people's convictions once their mind is made up, no matter how accurate or reputable the evidence countering their claims are. As a result, any education tactics must implement the "teach the teacher model". The information needs to come from an inside trusted source or they won't believe it.

4. Barriers for research: Information integrity is a complex and multidisciplinary problem with many technical, social, and policy challenges that requires the sharing of expertise, data, and practices across the full spectrum of stakeholders, both domestically and internationally. What are the key barriers for conducting information integrity R&D? How could those barriers be remedied?

Key barriers in conducting research in the information integrity space are the following:

- (1) Platforms closing or throttling data streams
- (2) Intense politicization of the topic (which makes people less willing to work on it)
- (3) Lack of local knowledge about what constitutes mis/disinformation in particular settings (e.g., when using memes that don't explicitly state the mis/dis)
- (4) Platform belief/perception that they can't do anything about it legally (I think they're wrong, but they often espouse this belief)
- (5) R&D on information integrity requires coupling across disciplinary boundaries beyond what is possible today due to the lack of, including but not limited to, appropriate organizations and promotion mechanisms.

5. Transition to practice: How can the Federal government foster the rapid transfer of information integrity R&D insights and results into practice, for the timely benefit of stakeholders and society?

We need research incentives to shift from identifying mis/dis-information to measuring mid/dis-information and understanding how to deploy interventions.

6. Relevant activities: What other research and development strategies, plans, or activities, domestic or in other countries, including in multilateral organizations and within the private sector, should inform the U.S. Federal information integrity R&D strategic plan?

One active, private sector activity that we would call to your attention is the Coalition for Content Provenance and Authenticity (C2PA, <https://c2pa.org/>). The C2PA is an international consortium consisting of technology providers and leading news organizations that is working to help combat the prevalence of misleading information online through the development of technical standards for certifying the source and history (or provenance) of media content.