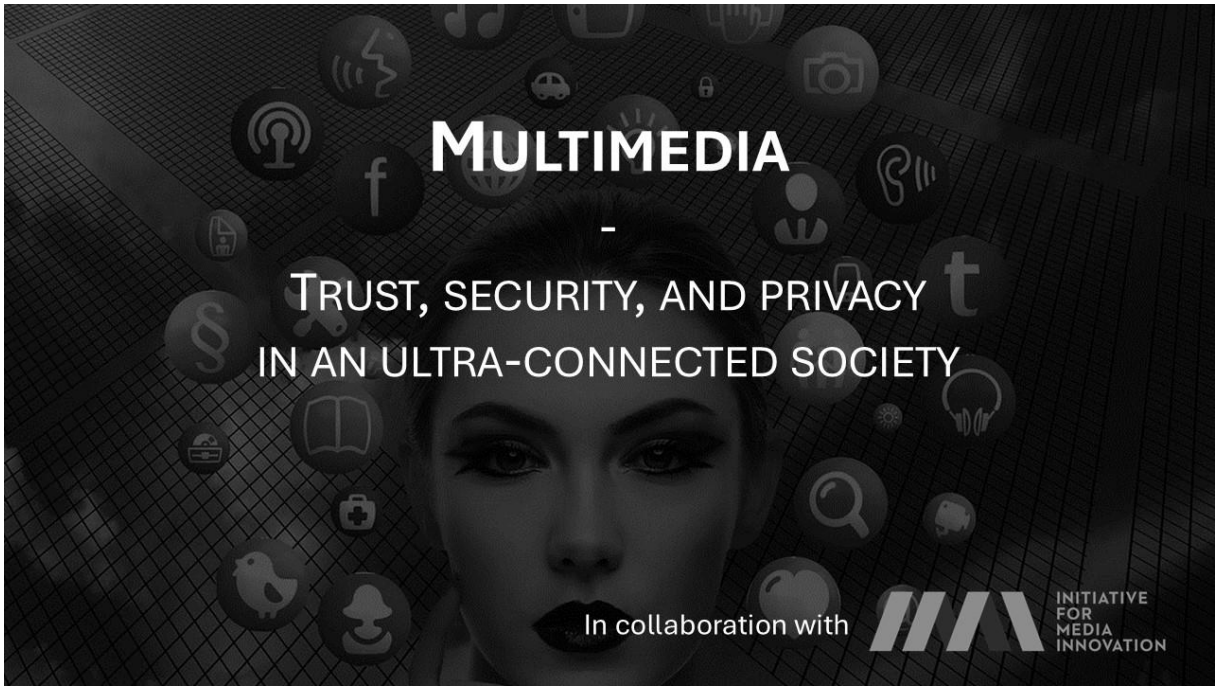
[seal]
EPFL . HEIG-VD . UNIL

CALL FOR PROJECTS #2

Opening 01.10.2024 | Closing 07.02.2025



This call aims to stimulate collaborative innovation to propose solutions that address the challenges of multimedia content security, from privacy to emerging threats associated with new technologies. It is carried out in collaboration with the Initiative for Media Innovation (IMI).

We invite university researchers, multimedia and press industry players, innovation stakeholders, and digital technologies experts to join forces to protect data and secure multimedia exchanges in a paradigm of profound change in information channels and human interactions.

CONTEXT AND CHALLENGES

For many years now, multimedia information has been gaining considerable importance, first with the advent of online media, then with social networks and connected objects, and finally with remote working and communication since the COVID crisis. Images, text and sound have become the main vectors of communication in society.

This paradigm shift has a direct impact on the notion of security at various levels. Cybersecurity therefore plays a key role in restoring trust, for example by preserving the confidentiality of content, guaranteeing its origin, enabling its traceability or certifying its integrity.

1

Protect privacy

In just a few years, our personal online exposure has increased massively, in direct correlation with the intensified use of social networks and other digital platforms. A significant part of an individual's private life is now accessible on the Internet (photos/videos, geographical location, CVs, etc.). Our biometric data, which is required by an increasing number of applications (in particular authentication by facial or voice recognition), is particularly sensitive. Robust measures to protect personal data, as well as intellectual and/or commercial property (e.g. photos and videos), are therefore essential.

2

Secure private communications

As technology continues to evolve, information channels and communications must become more secure. They must be able to guarantee authenticity and confidentiality at all times. This is especially true for the massive adoption of videoconferencing, but also more generally for email exchanges and other electronic interactions (especially in social networks and with connected objects). It is even a critical factor in the implementation of artificial intelligence (AI) models based on image analysis and classification for decision making (e.g. in autonomous vehicles).

3

Protect against the risk of public misinformation

More than ever, news producers and distributors must demonstrate their integrity and authenticity in the face of an influx of potentially manipulated information via electronic media, social networks, and other digital channels. For the majority of audiences, it is becoming increasingly difficult to discern truth from spin and form an objective opinion. Protecting against the risks of misinformation, in particular through the detection of deepfakes, is therefore a major challenge for civil society, requiring both computer science and social science skills.

OBJECTIVES

The objective of this call is **to explore new ideas and methodologies, to explore disruptive concepts and to develop innovative technical solutions that promote trust, security and privacy in the multimedia domain**, especially:

- Development of technological solutions to guarantee the security, integrity, authenticity and confidentiality of multimedia data (encryption, steganography, detection mechanisms and protection against falsification)
- Design of privacy protection mechanisms in a multimedia environment (data anonymization, consent management, minimization of personal data collection)
- Explore innovative approaches to detecting and countering potential multimedia threats (malicious content, misuse, cyber-attacks)

Expected projects include (but are not limited to) the following areas:

- Watermarking - and other measures to certify information at the source
- Detection, analysis and referencing of multimedia content manipulation - deepfakes (recognition algorithms, patterns, distribution/amplification modes)
- Characterization of attacks and development of protection for machine learning algorithms for the classification of images
- Biometric data management (facial recognition, behavioral biometrics)
- Voice forgery detection and countermeasures

CONTACT

If you have any questions or would like assistance in initiating a project, please contact:

Sandy Wetzel
[seal] Program Manager
+41 78 761 23 36
contact@seal-innovation.ch