

ExploreGen: Large Language Models for Envisioning the Uses and Risks of AI Technologies

Viviane Herdel¹, Sanja Šćepanović², Edyta Bogucka², Daniele Quercia^{2,3}

¹Ben-Gurion University, Negev, Israel

²Nokia Bell Labs, Cambridge, UK

³Kings College London, London UK

Abstract

Responsible AI design is increasingly seen as an imperative by both AI developers and AI compliance experts. One of the key tasks is envisioning AI technology uses and risks. Recent studies on the model and data cards reveal that AI practitioners struggle with this task due to its inherently challenging nature. Here, we demonstrate that leveraging a Large Language Model (LLM) can support AI practitioners in this task by enabling reflexivity, brainstorming, and deliberation, especially in the early design stages of the AI development process. We developed an LLM framework, *ExploreGen*, which generates realistic and varied uses of AI technology, including those overlooked by research, and classifies their risk level based on the EU AI Act regulation. We evaluated our framework using the case of Facial Recognition and Analysis technology in nine user studies with 25 AI practitioners. Our findings show that *ExploreGen* is helpful to both developers and compliance experts. They rated the uses as realistic and their risk classification as accurate (94.5%). Moreover, while unfamiliar with many of the uses, they rated them as having high adoption potential and transformational impact.

Introduction

In today's fast-paced tech world, balancing innovation with responsibility is essential (Sraml Gonzalez and Gulbrandson 2022; Owen and Pansera 2019). As Artificial Intelligence (AI) spreads across areas like healthcare and finance, it is crucial to understand its uses and potential risks relating, e.g., to data privacy, security, and fairness (Davenport and Kalakota 2019; Goodell et al. 2021; Dignum 2019; Tahaei et al. 2023). Business developers and engineers seek opportunities to employ the latest AI trends ahead of their competitors (Phaal, Farrukh, and Probert 2004), while researchers take part in a similarly fast-paced environment to publish their latest AI discoveries. In both roles, these AI practitioners are faced with increased need to envision potential uses, as well as risks and benefits of the technologies they are developing, and to produce AI impact assessment reports (Stahl et al. 2023). Given the increasing number of AI regulations (Smuha 2021), AI compliance experts also face the task of supporting their colleagues in assessing the regulatory risks and compliance of AI technologies. The process of cataloging AI uses and associated risks is both challenging and time-consuming (Moraes, Almeida, and de Pereira 2021; Liang et al. 2024; Hassel and Özkiziltan

2023). Recent research shows that AI developers struggle with detailing uses and impacts for model cards (Liang et al. 2024) and data cards (Yang, Liang, and Zou 2024), as well as for the broader societal impacts sections now mandated by some of the top AI conferences (Nanayakkara, Hullman, and Diakopoulos 2021; Prunkl et al. 2021; Ashurst et al. 2022). Recommendations to support AI practitioners with envisioning the impacts of their technology include encouraging reflexivity, including constructive and data-driven deliberation (Ashurst et al. 2022; Prunkl et al. 2021; Yang, Liang, and Zou 2024).

Our research responds to this challenge by exploring the use of Large Language Models (LLMs) to generate AI technology uses and their risk assessments based on the EU AI Act (European Commission 2024). This aims to support AI practitioners during the initial phases of the AI design process, including reflexivity, brainstorming, and deliberation. While LLMs have demonstrated utility in diverse applications (Gilardi, Alizadeh, and Kubli 2023; Wu, Terry, and Cai 2022; Dowling and Lucey 2023; Byun, Vasicek, and Seppi 2023), their suitability for two specific tasks—identifying potential uses of a given AI technology and conducting legal risk assessments of its uses—remains an open question. Our aim is not to produce an exhaustive list of uses for a given AI technology, nor to provide a definitive risk classification. Instead, we aim to investigate whether LLMs can generate outputs of sufficient quality to support AI practitioners in envisioning the impacts of their technology, particularly focusing on *less well-researched uses*. On one hand, LLMs might generate unrealistic use cases or ones that practitioners are already familiar with. On the other hand, the extent to which LLMs can accurately map legal regulations to specific AI uses, if at all, is yet to be substantiated.

This paper aims to evaluate LLMs for these specific goals. We explored them using OpenAI's GPT-4 (OpenAI 2023), making two main contributions (Figure 1):

1. We designed an LLM framework (*ExploreGen*) incorporating novel prompt elements—a set of curated *domains* to generate a variety of uses, and *risk concepts* proposed by Golpayegani, Pandit, and Lewis (2023), framing each use along these concepts for risk assessment (*UsesGen*). *UsesGen* classifies generated uses into realistic (existing and upcoming) and unlikely (hallucinations) with Chain-of-Thought (CoT) reasoning (Wei et al. 2022), retaining

only *realistic* ones. These uses are then classified into prohibited, high-risk, and limited or low-risk categories according to the EU AI Act (*RiskLabelling*). Additionally, we processed 3M Semantic Scholar papers, to uncover $\sim 12\%$ among the identified uses, which were overlooked by the scientific literature (*OverlookedFilter*).

- Using Facial Recognition and Analysis (FRA) technology as a use case, we *evaluated* our framework by assessing six aspects: (I) whether it generates realistic uses, (II) literature coverage of the generated uses, (III) familiarity of AI practitioners with these uses, (IV) adoption potential, (V) transformational impact, and (VI) accuracy of risk classification and perceived riskiness by AI practitioners.

To perform the evaluation, we conducted a scoping literature review, and nine user studies with 25 AI practitioners (12 AI developers and 13 AI compliance experts). We found that *UsesGen* generated realistic uses, covering 96% of the literature uses identified through the scoping review (I-II). AI practitioners reported low familiarity with the uses, especially the overlooked ones (III). They considered the uses somewhat to very likely to be adopted (IV) and to have a high transformational impact on business operations or people's lives (V). Compliance experts found that *RiskLabelling* correctly classified the risk of uses based on the EU AI Act with a 94.5% accuracy. Although over 50% of the FRA uses were classified as high risk or prohibited, AI developers, who were not presented with the classification, perceived most uses as only slightly risky for society and not at all for the environment. Lastly, thematic analysis of open-ended responses during in-person interviews revealed that both AI developers and compliance experts found *ExploreGen* helpful for ideation, brainstorming, and deliberation of AI uses and their risks and benefits. Compliance experts found it directly useful, while developers recommended adjustments to better suit their needs.

Background & Related Work

First, we present background on assessing impacts of AI technology, followed by a glimpse on the emergent AI regulations, and we finish with prior work leveraging LLMs for various tasks.

Assessing Impacts of AI Technology

AI impact assessments (AIAs) are recommended as a tool to recognize both the beneficial and adverse effects early in the AI technology development process, aiming to predict and evaluate the impact that new digital technologies have on all stakeholders. Stahl et al. (2023) reviewed literature and identified 38 proposed AIAs, including DataSheets for Datasets (Geburu et al. 2021) and methods inspired by environmental impact assessments (Calvo, Peters, and Cave 2020). However, despite the proliferation of proposed AIAs, developer teams often encounter difficulties initiating AI impact assessments (Buçinca et al. 2023) and require additional guidance throughout this process (Wang et al. 2023).

An important challenge faced by AI practitioners when performing AI impact assessments is mapping the intended and unintended AI uses (Liang et al. 2024; Yang, Liang, and Zou 2024; Prunkl et al. 2021). For example, recent research on 32K model cards posted on the HuggingFace platform (Liang et al. 2024) shows that while most cards detail *Training Information*, sections on *Intended Uses* and *Bias, Risks, and Limitations* have lower completion rates (17-23%). Similarly, Yang, Liang, and Zou (2024) found that in Data Cards also hosted on HuggingFace, the section on *Considerations for Using the Data* receives the lowest proportion of content (only 2.1% of the card's text length).

As another means of reflecting on potential positive and negative consequences of AI models, broader societal impacts are introduced as a requirement by leading AI conferences (e.g., the Conference on Neural Information Processing Systems (NeurIPS)) (Nanayakkara, Hullman, and Diakopoulos 2021). However, researchers also struggle with filling in such sections due to the inherently difficult nature of the task and high opportunity costs (Prunkl et al. 2021).

Conventional methods to understand the uses and scope of AI technology include systematic and scoping reviews, which are useful for mapping fields of study (Peters et al. 2015; Loncar-Turukalo et al. 2019). For instance, Moraes, Almeida, and de Pereira (2021) combined literature review with news media research to unveil FRA applications in (semi-)public spaces in Brazil and the associated risks. Similarly, Hupont et al. (2022) reviewed scientific papers and company portfolios to identify 60 facial processing applications, which were then assessed for risk level according to the EU AI Act. However, these methods, while insightful, are resource-intensive, demanding both time and expertise (Arksey and O'Malley 2005).

Moreover, even when the uses of AI are known, they can bring unanticipated challenges, from privacy and security issues (Li et al. 2023; Ekambaranathan, Zhao, and Van Kleek 2021) to distorting human beliefs (Kidd and Birhane 2023), excessive dependence that could diminish crucial human skills (Byun, Vasicek, and Seppi 2023; Lu and Yin 2021), and negative environmental impacts (Rillig et al. 2023), as well as impacts on human rights and society (Mantelero 2022). Anticipating such challenges and broader, systemic impacts of technology remains a significant challenge for AI practitioners (Prunkl et al. 2021; Yang, Liang, and Zou 2024; Weidinger et al. 2023).

Regulating AI

The pervasiveness of AI, along with the potential risks discussed above, has intensified calls for regulatory oversight (Tahaei et al. 2023; Borenstein and Howard 2021). The first binding regulatory response is the European Commission's AI Act (European Commission 2024), which aims to balance fostering innovation with protecting rights and societal values. The Act covers a spectrum from low-risk to prohibited AI applications, prohibiting those that can harm individuals or manipulate behaviors, such as social scoring by public authorities. It also allows for extending the scope of prohibited and high-risk uses, recognizing that AI regulations must evolve alongside technology (Hutson 2023).

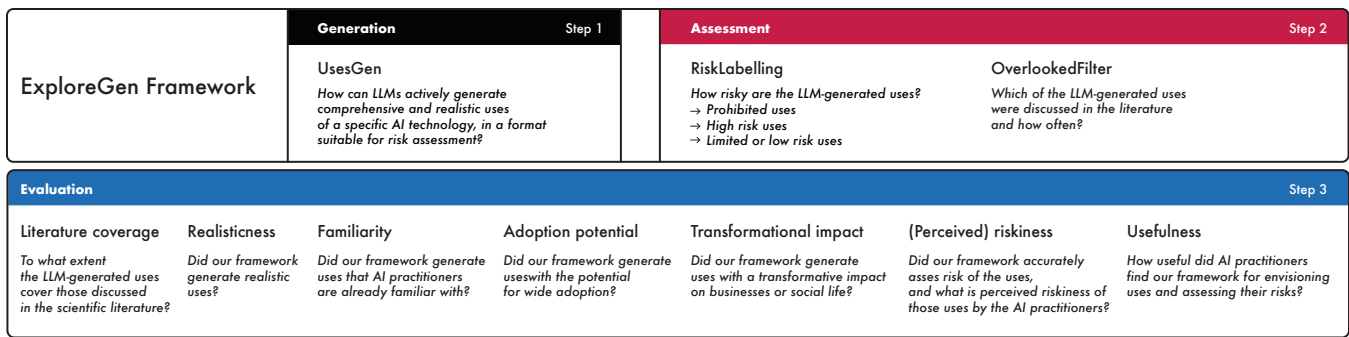


Figure 1: Our methodology consists of three steps. In the first two steps, *ExploreGen* performs (i) *generation (UsesGen)* of various uses for a given AI technology, and their (ii) *assessment (RiskLabeling, OverlookedFilter)* in terms of the risks based on the EU AI Act, and determining whether they are discussed or overlooked in previous literature. In the last step (iii), we did the *evaluation* of the generated uses and their risk classification, including the realisticness of the uses, risk assessment accuracy, and usefulness for AI practitioners in envisioning the impacts of AI technology.

Other regulatory frameworks include the US Office of Science and Technology Policy (OSTP) Blueprint for an AI Bill of Rights, China’s Interim Measures for the Management of Generative AI Services, and the UK’s pro-innovation approach to AI regulation.

To sum up, the dynamic nature of AI poses a challenge in its impact assessment, particularly in identifying its myriad uses and ensuring thorough risk assessments. We propose to leverage LLMs to partly tackle these challenges.

Large Language Model Applications

LLMs have already demonstrated their usefulness in a variety of tasks. These range from text annotation (Gilardi, Alizadeh, and Kubli 2023) to assisting with creative and argumentative writing (Lee, Liang, and Yang 2022) and potential for providing help for mental health issues (Sharma et al. 2023). LLMs offer insights that surpass general public knowledge (Gilardi, Alizadeh, and Kubli 2023), show promise in human-AI co-creation processes (Wu, Terry, and Cai 2022; Lee, Liang, and Yang 2022), brainstorming assistants (Lukowicz et al. 2023; Bouschery, Blazevic, and Piller 2024), and have the potential to support *interpreting regulatory texts* (Zheng et al. 2023; Cui et al. 2023).

To achieve the desired output from LLMs, it is important to employ best practices in prompt engineering, such as Chain-of-Thought reasoning, using appropriate roles, and providing cues and examples to guide the model’s output (Wu, Terry, and Cai 2022; Shieh 2023). However, LLMs also introduce their own AI risks, including biases associated with the training data (Luccioni et al. 2024) and hallucinations (Mittelstadt, Wachter, and Russell 2023), which need to be carefully considered in each application.

Methodology

For our framework’s development and assessment, we focused on Facial Recognition and Analysis (FRA), a well-established yet controversial technology due to its known risks (Zhang, Feng, and Sadeh 2021; McClurg 2007), and a contentious topic during the development of the EU AI Act

(Hupont et al. 2022).

Designing ExploreGen

We selected GPT-4 due to its top-ranking performance, as shown in leaderboards (LMSYS 2024).

Generating Uses (UsesGen). To generate a list of various uses (Figure 1, Framework, Step 1), we specified five elements in UsesGen (Appendix, Figure 4): system role, instructions, risk concepts, definitions of being realistic, domains, and examples.

The *system role* has been shown to improve the quality of the output, as it allows to generate content from specific perspectives (Giray 2023). We assigned the role of a “*Senior [Technology X] Specialist and Evaluator*” and described its main tasks as “*reviewing, and cataloguing the diverse applications and use cases of [Technology X] across multiple domains, and conducting exhaustive research and analysis*”.

We then followed with the three-part *instruction*: (i) to create a comprehensive and self-explanatory JSON (JavaScript Object Notation) list detailing particular use cases or applications of [Technology X], (ii) to provide precise descriptions for each concept, and (iii) to categorise the LLM-generated uses into 1) *already existent*, 2) *upcoming*, and 3) *unlikely*, along with a one-sentence justification for each use categorization (enacting the *CoT reasoning*).

We asked for each use to be generated along the five concepts proposed by Golpayegani, Pandit, and Lewis (2023):

1. *Domain*: “The area or sector the AI system is intended to be used in” (e.g., education).
2. *Purpose*: “The objective that is intended to be accomplished by using an AI system” (e.g., attendance tracking).
3. *Capability*: “The capability of the AI system that enables the realisation of its purpose and reflects the technological capability” (e.g., identify students’ faces and match them with database).
4. *AI user*: “The entity or individual in charge of deploying and managing the AI system, including individuals,

organisations, corporations, public authorities, and agencies responsible for its operation and management” (e.g., schools).

5. *AI subject*: “The individual directly affected by the use of the AI system, experiencing its effects and consequences. They interact with or are impacted by the AI system’s processes, decisions, or outcomes” (e.g., students).

To aid the realism categorisation, we also provided the *definitions* of the three categories of being realistic. AI-ready existing uses were defined as currently implemented and well-established uses. Upcoming uses were defined as being under current development, being researched, or subject to discussions without being implemented or being severely limited in practice due to various reasons. Lastly, unlikely uses, introduced to capture hallucinations, lack value, usability, applicability, or practicality, or are deemed unnecessary, impossible, incoherent, or unrealistic.

To further guide UsesGen we requested the AI technology uses across a broad set of *domains*. Without such a request, the uses generated by the LLM would encompass the most common and well-known FRA uses, since LLMs suffer from exposure bias (Wu, Terry, and Cai 2022). The domains served as a *cue* in our prompt. Our procedure for listing a broad set of domains was as follows. First, domains were derived from the EU AI Act’s Annex III (e.g., “Education and vocational training”), along with 32 domains that were not explicitly listed but were mentioned in the EU AI Act text or its Amendments (e.g., “Social Media” from Amendment 51 stating: “*The indiscriminate and untargeted scraping of biometric data from social media [...] add to the feeling of mass surveillance [...]*”). Moreover, we derived additional domains from a focus group using a think aloud protocol ($N=8$) to ensure capturing all significant domains beyond the EU AI Act. The session was with our research group (3F, 5M, mean age: 31.8, SD : 6.74, range: 22-45). We used a Miro board and asked the participants to think of domains that affect their lives along the five levels of the Social-Ecological Model (Golden et al. 2015): individual, interpersonal, institutional, community, and public policy. This resulted in an additional 6 domains that were not yet covered by the previous list of 40 domains, resulting in the final 46 diverse domains (Appendix (B)).

To complete the prompt, we carefully crafted five *examples* (employing *few-shot* learning (Brown et al. 2020)) striking a balance between providing a diverse range of examples and keeping the prompt at a manageable context length (Liu et al. 2024). The output also requires the label for the realism of the use. For example, “FRA for medical diagnosis” was categorised as an *upcoming* use, along with the justification saying that it *has the potential to revolutionise healthcare, yet successful integration depends on resolving privacy, regulatory, and trust-related issues*. We placed the examples section at the end of the prompt, as examples can not only illustrate the desired input-output relationships, but also aid the model’s context comprehension and response expectations (Brown et al. 2020).

Assessing the Risk of Generated Uses (RiskLabelling).

To enable risk assessment as per the EU AI Act (Figure 1, Framework, Step 2), we specified five elements (Appendix, Figure 5): system role, instructions, legal documents, placeholder for a list of uses, and output structure.

We started the prompt by selecting the *system role* of an “*Experienced Judge who works in the field of AI technology regulation*”, and described the role further: “*You are thoughtful, decisive, experienced and conscientious. You have access to the entirety of the EU AI Act*”.

We then provided the *instructions* to classify the uses by utilising the *CoT reasoning* by requesting to first expand the concise FRA use into a description of a hypothetical AI system that employs it. We then followed with the requests to consider the EU AI Act and its amendments (European Commission 2024) provided in *input*, and to classify the system as “prohibited”, or “high risk”, or, otherwise, as “limited or low risk”.

The prompt was then provided with the *placeholder* for AI technology uses for which the risk assessment should be performed.

Finally, we requested the *output structure* of the risk classification to encompass:

1. *Description*: Provides a clear understanding of the intended use of the AI system.
2. *Classification*: Outcome of the classification which can be either prohibited, high risk, or limited or low risk.
3. *Relevant Text from the Act*: If applicable, a quote from the EU AI Act is included, along with a relevant amendment or section to provide legal context.
4. *Reasoning*: Explanation that rationalises the specific risk classification of the inputted AI use.

Table 1: LLM-generated uses overlooked by the research literature. For full details of these uses, see Appendix, Table 4.

Use ID.	Use Description
27.	Validate remote worker identity online.
52.	Recognize customers, tailor services.
68.	Identify watchlisted individuals at borders.
69.	Verify asylum seeker identities.
70.	Prevent voter fraud via identity verification.
80.	Authenticate energy facility personnel access.
83.	Verify military personnel identities.
84.	Identify threats in crowds by military.
88.	Identify citizens for personalized services.
91.	Secure embassies by identifying visitors.
98.	Authenticate emergency responders’ identities.
104.	Verify cargo access by authorized personnel.
108.	Control access to restricted urban areas.
114.	Verify access to protected environmental areas.
118.	Identify illegal loggers.
120.	Verify access to climate-sensitive areas.

Assessing the Literature Coverage of Generated Uses (OverlookedFilter). To assess which of the LLM-generated uses were discussed in the literature (Figure 1, Framework, Step 2), and possibly uncover overlooked ones by the literature, we collated all the 200M papers from Semantic

Scholar’s May 2023 dump.¹ We then filtered the papers to those being written in English, and having both the title and abstract fields available, resulting in 3M papers.

Next, we embedded the `title + abstract` field for each of the articles, as well as the description of each of the LLM-generated use using *all-mpnet-base-v2* sentence-transformers (Reimers and Gurevych 2019) model.² This model is trained using a self-supervised contrastive learning, by fine tuning the pretrained *microsoft/mpnet-base* model on above 1 billion sentences. Upon pairing each use with the paper with the maximum similarity of their embeddings, we then manually explored which similarity threshold will yield use-paper pairs such that the paper’s abstract indeed discusses the use. We explored {95th, 99th, 995th, 999th} percentile thresholds, until we concluded that the 999th percentile one yielded 3,295 papers, which indeed discussed paired FRA uses.

The top frequent venues in which these papers are published include: arXiv.org, International Journal for Research in Applied Science and Engineering Technology, IEEE International Conference on Systems, Man and Cybernetics, ACM Multimedia, Interspeech, PLoS ONE, IEEE/ACM International Conference on Human-Robot Interaction, and Computer. The most commonly discussed uses are: *Secure access control, use #1* discussed by 291 articles, *Detecting driver fatigue through facial analysis, use #134* discussed by 251, and *use #60, Using diverse facial data to refine algorithms*, discussed by 189 articles.

Evaluating ExploreGen

This section outlines the process of evaluating our ExploreGen framework (Figure 1, Framework, Step 3). The goal of our framework was to generate realistic uses of a given AI technology, such that AI practitioners are not familiar with all of them, and to accurately classify their risks based on the regulation. Moreover, the generated uses should exhibit potential for adoption and transformational impact.

To ascertain the effectiveness of the framework at meeting this goal, our evaluation ought to answer seven questions:

- I. *Literature coverage*. To what extent the generated uses cover those discussed in the scientific literature?
- II. *Realisticness*. Did our framework generate realistic uses?
- III. *Familiarity*. Did our framework generate uses AI practitioners are familiar with?
- IV. *Adoption potential*. Did our framework generate uses that have a potential for adoption?
- V. *Transformational impact*. Did our framework generate uses that have a transformation impact?
- VI. (*Perceived*) *riskiness*. Did our framework accurately assess risk of the uses, and what is perceived riskiness of those uses by the AI practitioners?
- VII. *Usefulness*. How useful did the AI practitioners find our framework in assisting with their tasks of envisioning AI uses and assessing associated risks?

¹api.semanticscholar.org/api-docs/datasets

²huggingface.co/sentence-transformers/all-mpnet-base-v2

Metrics. We then defined six quantitative and one qualitative metric to answer these questions.

The first metric assessed the *coverage* of the generated use cases in relation to those discussed in the literature. It was measured as the percentage of matches with the ground truth (GT), which we derived from a scoping review of FRA use cases (Appendix C). Two authors independently conducted a manual assessment, categorizing each generated use case as either matching or not matching the ground truth list.

The second metric assessed the *realisticness* of the generated uses. We measured it by calculating the agreement between the realism labels assigned by the LLM and those given by the participants in the user study.

The third metric assessed participants’ *familiarity* with the generated uses. It was measured through a question: “*How frequently do you encounter references to this use in your professional life?*” evaluated on a 7-point Likert scale from ‘rarely’ to ‘always’.

The fourth metric assessed practitioners’ perceptions about the real-life *adoption potential* of the LLM-generated uses. It was measured through a question: “*How likely it is that this use will be widely adopted in the near future?*” evaluated on a 7-point Likert scale from ‘very unlikely’ to ‘very likely’.

The fifth metric assessed AI practitioners’ perceptions of the potential *transformational impact* of the LLM-generated use cases. It was measured by asking, “*How likely is it that this use will fundamentally change the way businesses operate or people live?*”. Participants rated this on a 7-point Likert scale from ‘very unlikely’ to ‘very likely’.

The sixth metric assessed AI practitioners’ perceptions of the *riskiness* of the use cases in terms of their potential societal and environmental adverse impacts. It was measured by asking both AI developers and compliance experts to answer how risky do they consider the use “*for society as a whole*” as well as “*for the environment*”. These two questions were rated on a 7-point Likert scale from ‘not risky at all’ to ‘unacceptably risky’. Additionally, to validate *RiskLabelling*’s classification outputs, we provided the compliance experts with both the classification and the LLM’s justification and measured their agreement. If they disagreed with the classification, they could select the correct classification (including the option of ‘insufficient information to assess the use’). If they disagreed with the justification, they could provide their own reasoning.

The last, seventh metric was about the *usefulness* of our framework, captured through three open-ended questions: “*How useful is this framework for envisioning uses of technology?*”, “*How useful is this framework for understanding the risks and benefits of each use?*”, and “*At what stage in your assessment process would you use this framework?*” .

Setup. To derive the first metric (*literature coverage*), we performed a scoping review. To derive the remaining six metrics (*realisticness, familiarity, adoption potential, transformational impact, perceived riskiness, usefulness*), we conducted nine user studies with 25 AI practitioners in total (12 AI developers, and 13 AI compliance experts).

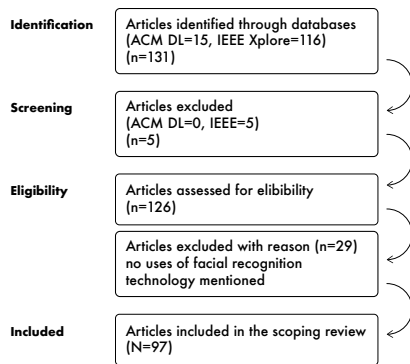


Figure 2: *The scoping review*: identification, screening, and assessment for eligibility of articles. Starting with 131 initial papers identified, a total of 97 were included. From these papers, 75 unique FRA uses were identified (Appendix C).

Scoping Review. To obtain a list of a FRA uses discussed in the literature, we performed the scoping review in accordance with the 5-stage guidelines (Arksey and O’Malley 2005):

1. *Identifying research questions.* RQ: “What are the documented, researched, or proposed uses of FRA as found in the literature?”
2. *Identifying relevant articles.* In consultancy with the research team, we selected the ACM Digital Library (<https://dlnext.acm.org>) and IEEE Xplore (<http://ieeexplore.ieee.org>) as our databases, which correspond to the main Computer Science and Engineering digital libraries, likely to cover a broad spectrum of research on FR technology. We used the following Query (Q) = [[Title: “face recognition”] OR [Title: “facial recognition”]] AND [Full Text: “use case*”] (Figure 2, *Identification*).
3. *Selecting articles.* We included peer-reviewed articles as well as larger scholarly works, such as extended abstracts (e.g., posters and demos) and workshop papers. All selected works are referred to as *articles*. For all identified articles, we applied the following inclusion criteria: (1) written in English and (2) describing, studying, or envisioning at least one use of facial recognition technology. In the initial search, 131 articles were identified from the ACM and IEEE databases. As no duplicates were found, all 131 articles were screened based on titles and abstracts. Five articles were removed as they did not discuss an FRA use (Figure 2, *Screening*). Subsequently, 126 articles were assessed for eligibility based on their full text (Figure 2, *Eligibility*), resulting in a final selection of 97 relevant articles (Figure 2, *Included*). The lead author performed the article selection process.
4. *Charting the data.* The lead author began reading the articles and simultaneously developed a coding system for the FRA uses described, studied, and envisioned in the articles. As the lead author read the articles, they color-coded the FRA uses and extracted them. Each time a new FRA use was identified, it was added to the coding sys-

tem. Any ambiguities—though rare due to the straightforward nature of the FRA uses mentioned—were discussed and resolved between the lead and second author.

5. *Collating, summarising, and reporting results.* The scoping review resulted in 97 articles from which we identified 75 unique uses of FRA, listed in Appendix C.

User Studies with AI Practitioners. We conducted seven in-person studies involving 3 AI developers (30 minutes each) and 4 AI compliance experts (45 minutes each), complemented by two online studies on Prolific: one with 9 AI developers, and another one with 9 AI compliance experts.

The in-person studies consisted of four steps. First, we asked participants about their current practices and challenges in envisioning AI technology uses and their associated risks. Second, we presented an interactive list of 138 uses and tasked them with selecting one project that balances being interesting to develop and adhering to the company’s code of conduct (Figure 6A), followed by questions on the usefulness of this list for envisioning technology uses and understanding the risks and benefits. Third, we presented 16 interactive assessment cards for overlooked uses and tasked them with annotating the uses for realismness, familiarity, adoption potential, transformational impact, and perceived riskiness (Figure 6B). AI compliance experts also evaluated the *RiskLabelling* classification and justification, making corrections if necessary (Figure 6C). This allowed us to compare perceived use riskiness between developers and compliance experts. Finally, we asked participants about the framework’s usefulness for envisioning technology uses, understanding risks and benefits, and identifying the stage in their assessment process where they would use this framework. Each of the 16 uses was annotated by 7 different AI practitioners: 3 AI developers and 4 AI compliance experts.

The online studies used a custom web-based survey consisting of five pages. The first page outlined the study’s description and tasks for crowdworkers: read the definitions of ‘risky’ uses and annotate each use for realism, familiarity, adoption potential, transformational impact, and perceived riskiness. AI compliance experts were also asked to agree or disagree with the *RiskLabelling* classification and justification, and make corrections if necessary. The second page provided definitions of risky uses according to the EU AI Act. The third and fourth pages presented assessment cards for 46 uses (23 per page) with input boxes for annotations (Figure 6A,B). The final page included a confirmation note and redirected participants to Prolific. Each of the 138 uses was annotated by 6 different AI practitioners: 3 AI developers and 3 AI compliance experts.

To ensure response quality, we conducted two attention checks during the studies and implemented two deliberate survey design features. First, after reading task instructions, participants encountered one of the two attention-check sentences: “When asked for your favorite color/city, you must select “Blue/Rome””. We also included one prohibited use labelled as “low risk” with a false justification mimicking text from the EU AI Act. Participants had to correctly respond to two out of these three checks. Second, we disabled past-

ing from external sources and editing previous responses to ensure original and thoughtful answers.

Participants. For our studies, we recruited participants and surveyed them across two cohorts: *a)* AI developers and *b)* compliance experts.

For the in-person studies, we recruited participants through an internal mailing list at a large tech company, and our professional networks. We asked for individuals currently developing AI systems using machine learning, computer vision, and image recognition. To recruit AI compliance experts, we sought individuals familiar with the EU AI Act, experienced in reviewing AI use cases, and involved in at least one ongoing AI impact assessment project.

For the online studies, we recruited participants from Prolific, controlling for their roles in the organization, the frequency of AI use in their jobs, fluency in English, and geographic location. To recruit AI developers, we selected participants who likely contribute to developing AI systems as part of their software engineering roles, using AI daily. To recruit compliance experts, we looked for participants likely involved in revising AI systems as part of their legal roles, using AI at least 2-6 times a week. We limited our participant pool to individuals residing in the European Union. All Prolific participants were paid an average of \$12 USD/hour. **Analysis.** We performed both quantitative and qualitative analyses. For the quantitative analysis, we measured the frequencies across six metrics: coverage, realism, familiarity, adoption potential, transformational impact, and perceived riskiness. For the qualitative analysis, we thematically analyzed responses to open-ended questions (Saldaña 2015; Miles and Huberman 1994; McDonald, Schoenebeck, and Forte 2019; Braun and Clarke 2006) to understand factors influencing the framework’s usefulness for envisioning technology uses, assessing risks and benefits, and determining the appropriate assessment stage for its application.

Evaluation Results

UsesGen, using FRA technology as input, generated 138 uses listed in Appendix D, Table 4. According to its own realism label, 8 (6%) of the uses were deemed unlikely (e.g., *FRA to track the carbon footprint of individuals, use #119*, as it is unlikely to be adopted, and *detecting plant diseases and pest infestations, use #50*, as it does not employ the capabilities of FRA).

RiskLabelling classified 10 (7%) uses as prohibited, 66 (48%) as high risk, and 62 (45%) uses as limited or low risk. Example *RiskLabelling* outputs for one use per each class are shown in Appendix, Table 3.

OverlookedFilter identified 16 out of the 138 LLM-generated uses that were not discussed in any of the 3 million Semantic Scholar papers we analyzed. These uses, which we term overlooked, are presented in Table 1. This indicates that while these uses are likely mentioned in news, press, or social media (and thus included in the LLM training data), they have not yet been the focus of in-depth scientific research.

I. Literature coverage. The uses were expressed differently between the GT list (Appendix C) and the LLM-generated list (Appendix D, Table 4). In the GT list, they are written as

single sentences mainly describing the purpose, whereas in the LLM-generated list, they always follow a structured format based on the 5 risk concepts (e.g., AI domain, AI user). Therefore, we employed a relaxed matching approach, allowing us to count two uses with different levels of generality as a match (e.g., *detect fatigue in individuals, GT-use #69* was matched with *improving driver safety by detecting driver fatigue through facial analysis, use #134*).

The LLM-generated list covered 96% of the literature-derived GT uses with the only 3 GT uses not found in the LLM-generated list being: *Provide real-time information about visitors in high-profile buildings, GT-use #5*, *Help people recognise faces by using smart glasses to display names and social network activities of identified people, GT-use #72*, and *Facilitate tourists in meeting new people, GT-use #74*.

Given the relaxed approach we applied, the high matching rate between the two lists reflects the LLM-generated list’s scoping coverage of various uses discussed in the literature rather than comprehensively covering all possible uses. Given the many contexts for each use (e.g., various subjects, domains, or locations), comprehensive coverage is practically unattainable.

II. Realisticness. After excluding the 8 uses labeled by the LLM itself as unrealistic, the majority agreement across the participants in different user studies was that the remaining 130 uses were all realistic. Of these, 91 uses (70%) were labeled as already existing, and 39 (30%) as upcoming (e.g., *recognizing signs of distress or confusion for elderly care assistance, use #6* and *facilitating non-verbal communication by interpreting facial expressions and gestures for non-verbal individuals, use #77*).

The analysis of unrealistic uses revealed that some domains were more prone to hallucination, such as “Agriculture and Farming” or “Environment and Sustainability.” Given that FRA has fewer applications in these domains, asking the LLM to generate uses in these areas led to hallucinations. These domains were included because they are mentioned in the EU AI Act and hold potential significance for other AI technologies (e.g., Earth Observation), where they might not lead to hallucinated uses.

III. Familiarity. As shown in Figure 3, both AI developers and compliance experts demonstrated low familiarity with the uses produced by *UsesGen*. Over 50% (48%) of these uses were reported by developers (compliance experts) as rarely encountered in their professional lives. For the overlooked uses, developers reported rarely encountering 60% of these, while compliance experts reported rarely encountering even 75%. The chi-squared test results confirmed that the distributions of familiarity scores significantly differ between all uses and overlooked uses, validating the ability of our *OverlookedFilter* to identify less well-known and understudied uses. The distribution of familiarity scores did not differ statistically significantly between the cohorts of AI developers and compliance experts.

IV. Adoption potential. AI developers thought that most of the uses are ‘somewhat likely’ (~27% of the uses) or ‘very likely’ (~25% of the uses) to be adopted, though the ratio

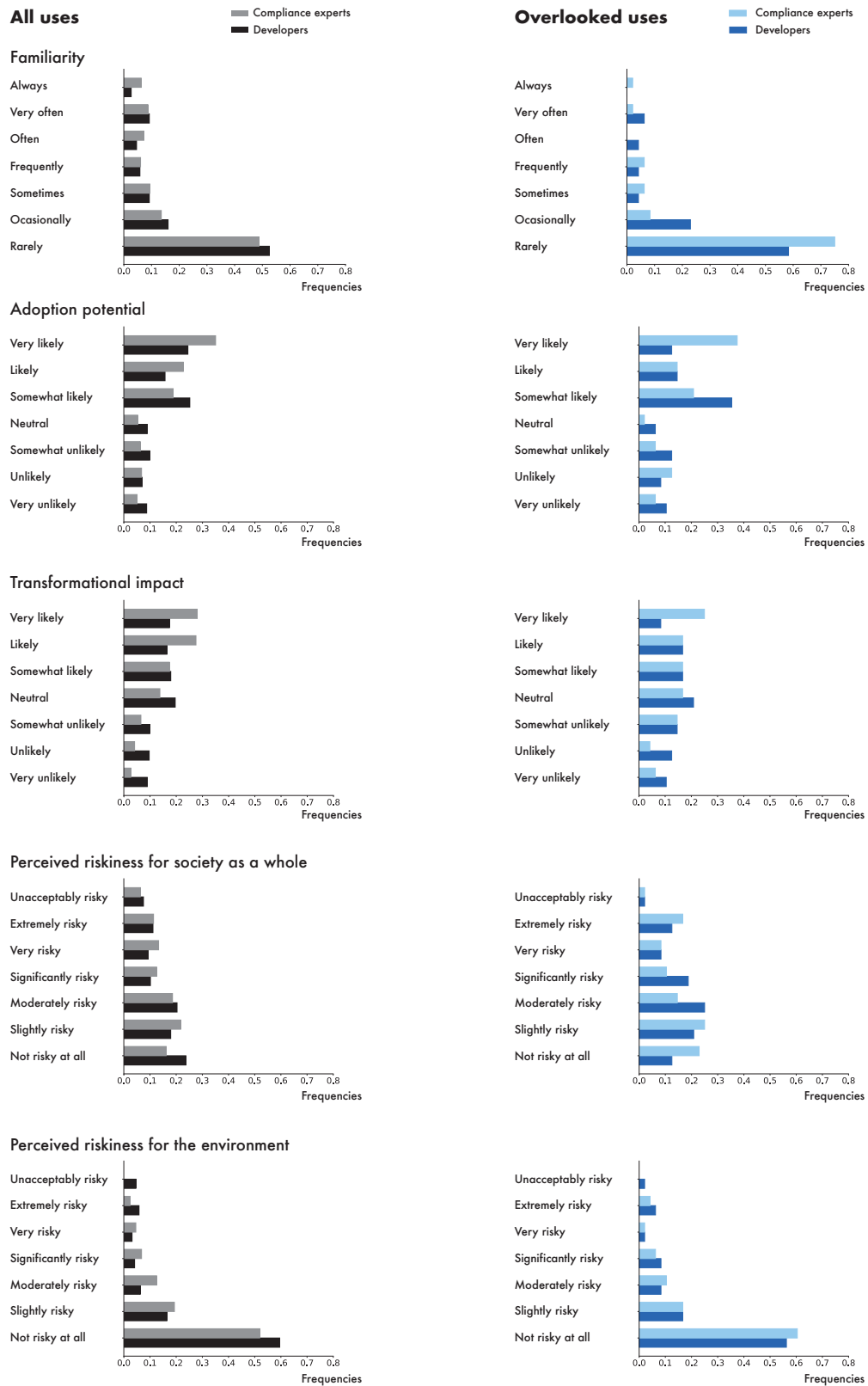


Figure 3: Evaluation results for the five quantitative metrics: familiarity with the use, its adoption potential, transformational impact, and perceived riskiness for society as a whole and for the environment.

of the ‘very likely’ ones was smaller for the overlooked uses (<15% of the uses). Compliance experts were, interestingly, scoring most of the uses, including the overlooked ones, as ‘very likely’ (>35% of uses) to be adopted. In this case, a chi-squared test results confirmed that the distributions of scores for adoption potential significantly differed between the two cohorts, with compliance experts generally giving higher scores.

V. Transformational impact. Developers were slightly more conservative in estimating the potential for transformative impact of the uses (Figure 3), assigning the largest proportion of uses a ‘neutral’ score (~20%). In contrast, compliance experts gave the highest proportion of ‘very likely’ scores (>25% of the uses) for both all and overlooked ones. Similarly as for the adoption potential scores, a chi-squared test results confirmed that the distributions of scores for transformational potential significantly differed between the two cohorts.

VI. (Perceived) riskiness. Each use was rated by three compliance experts. To obtain the ground truth label, we required that at least 2 of the 3 labels were aligned. By comparing these ground truth labels with the *RiskLabelling* labels, we found that 94.5% of the uses were correctly classified, with an almost perfect Cohen’s Kappa agreement of 92.2%. However, the inter-rater agreement among the three annotators was only moderate, with a Fleiss’ Kappa score of 49.1%, suggesting the task is challenging and that participants might have defaulted to the provided labels.

For example, participants disagreed with the LLM’s limited or low-risk classification for uses such as *verifying the identity of customers during transactions by banks, use #19*, and *identifying obstacles and people to avoid collisions by robots, use #56*. For *use #19*, they commented that it should be high risk due to the “*high chance for fraud*” and the possibility that the “*AI system could see the PIN of the bank card!*”. For *use #56*, two annotators voted for a high-risk label because “*in the case of misuse or malfunctioning, the AI could lead to serious harm for individuals*” and “[...] *put human lives at risk.*”

On the other hand, the participants did not agree with the high-risk classification for *assisting law enforcement agencies in criminal investigations by identifying suspects in video footage, use #85*. Two of them thought this use should be classified as *prohibited* in the EU, as it could lead to violations of privacy rights. The LLM did not classify it as such because the identification from footage is not in real-time, which is a requirement for prohibited uses specified in Article 5(1)(d). The third annotator, however, suggested downgrading the risk classification to limited or low risk because the use is “*necessary to provide proof and existence of criminal activities and facilitate law enforcement work*”. These examples demonstrate the subtleties in the risk assessment task, including the interpretation of the use context and the annotators’ personal viewpoints (Hupont et al. 2022), which partly explain the lower inter-rater agreement among our participants.

As shown in Figure 3, developers thought that most of the uses are only ‘slightly’ to ‘moderately risky’ for society

(approximately 20-25%), and not at all risky for the environment (approximately 50-60%). This contrasts with our risk classification finding that over 50% of the uses are either high-risk or prohibited according to the EU AI Act. These results highlight the challenge developers face in identifying and classifying the riskiness of AI uses.

VII. Usefulness. Finally, we studied the extent to which the two cohorts of AI practitioners found our framework useful in assisting with tasks such as envisioning AI uses and assessing associated risks.

AI compliance experts found *ExploreGen*’s output particularly useful. For example, L01 mentioned that a tool “*classifying [uses] in different ways and offering various uses of those [technologies], would be very useful in my job, [...] because it would help me look at things in a different way.*” L03 stated, “*I enjoyed it [...] I think it’s really helpful to kind of envision what will be the future use of AI and then think about how it will impact society and the environment. I think it’s a good exercise for someone working in the tech space in general,*” and “*... it will also be useful for people who want to understand the technology, like people impacted by the technology and the public.*” One participant from a major tech company developing FRA technologies expressed excitement upon discovering uses they are currently working on, particularly in risk and compliance assessment. They also found inspiration for new potential use cases, stating, “*We are putting more effort into going into the [domain X], and that could be a good use.*” L04 was particularly engaged with the risk-classification output provided by our tool. For instance, they focused on the use *identifying personnel by logistics companies to improve the efficiency of cargo handling, use #104*, and agreed with the low-risk classification. They noted that “[*A major company*] *has just gotten a judgment in its favor that very far-reaching analytics in its plants in [country Y] are permissible.*”. L03 was also inspired to think about the risks of the presented uses. They deliberated about the use *verifying patient identity in medical settings, use #10*, which is classified as low risk, but they thought it could incur many risks as “*services like this [...] can be exclusionary to certain, especially marginalized communities.*” They concluded, “*I would look into developing this, but I would consider this a high-risk use depending on the context and on the decision that’s being made by verifying.*”

AI developers, on the contrary, initially struggled to identify the application of our tool in their everyday work. While interested in exploring the presented uses, they frequently asked for more details and insights on specific uses. For instance, D02 expressed feeling overwhelmed by the comprehensive list of uses: “*I imagine [I am] developing that, and put a lot of cognitive load in each case and then imagining how it will work and how it will be developed.*”. During the interviews, it became clear that developers, especially those working on business products, have less opportunity to use a tool like *ExploreGen* because they typically do not engage in extensive brainstorming and reflexivity. Instead, they usually receive well-defined uses to develop. For example, D03 commented, “*I’ve been working with products and generally you start with a use that you want to develop [...] and*

then you work backwards and maybe a technology is not useful for that particular problem.” D03 also stated, “For most of the people I speak with, it seems like more of an afterthought than like an active design. [You think] what could be the risks kind of post hoc?” They added, “But I think people are generally getting a little bit better at that now because I think people are seeing that AI is progressing quite fast...” For these reasons, developers appreciated the color-coding of the use risk levels, as it provided a quick overview of the more or less risky domains, contexts, and uses. One participant noted surprise at seeing a similar use having different risk levels in two domains, finding the tool helpful for educating them about the EU AI Act and its domain-based risk classification. D01, who holds the most senior role among the developer participants, stated: “[We] have a brainstorming session on first of all, understanding if AI is really needed to solve the problem or not[...]” They added about our tool: “It will be very helpful for me or someone in my team to get a first sense of the risks involved...” Generally, developers preferred the second task in the study, where they could focus on a subset of uses and scrutinize them in detail, as this aligns more closely with their job responsibilities. Additionally, those in senior roles and closer to R&D found our tool more useful for brainstorming and deliberation tasks compared to junior developers and those working in business production.

Both AI developers and AI compliance experts agreed that a tool like ours would be most useful during the *design* stage of AI development. Moreover, several participants indicated they would use it throughout *all* stages, as noted by L4: “I don’t think one stage is more important than the other. I think there are different risks at different stages.”

Discussion

The findings from nine user studies revealed the potential of our proposed LLM framework *ExploreGen* to facilitate reflectivity, ideation, and deliberation for both AI developers and compliance experts—tasks that are increasingly essential but often challenging to perform (Liang et al. 2024; Prunkl et al. 2021). Our tool contributes to the existing body of research calling for (Sherman and Eisenberg 2024) and exploring (Buçinca et al. 2023; Wang et al. 2024) LLMs as a means to support responsible AI design.

Implications

Brainstorming in AI Developer Teams. *ExploreGen* successfully generated realistic uses that practitioners were not very familiar with, many of which were rated as having high adoption potential and transformational impact. Developers found the overview of uses contextualized across various domains, along with their risk levels, to be informative. Some saw the tool’s value during brainstorming meetings while deliberating on which directions for technology applications to pursue. Additionally, they expressed interest in a tool with a more in-depth analysis of specific uses, allowing to break down the associated risks of the use they are developing and be informed about similar risks faced by different uses.

Bridging Risk Perception with Compliance. Compliance experts agreed with the risk classifications provided by

RiskLabelling, though they noted that subtle changes in the context of use might alter the classification level. Despite more than 50% of the FRA technology uses being classified as high risk or prohibited, practitioners perceived them as mostly only slightly risky for society and not at all for the environment. However, due to the size of the datasets and computational demands, energy consumption is becoming an important consideration for FRA technology (Hassel and Özkiziltan 2023), highlighting a disconnect in AI practitioners’ understanding of all the technology’s impacts.

Data-driven Deliberation for Compliance Experts. Compliance experts saw more direct applications of *ExploreGen* in its current form for their work, as they often explore various (often unintended or unexpected) contexts of use for a given technology. They found the tool very helpful for this task. They also appreciated the breakdown of uses across various domains and risk levels and wanted features allowing for additional breakdowns (e.g., according to the subjects or types of risk).

Limitations and Future Work

LLM Method Shortcomings. The use of LLMs presents four main challenges. First, the generated uses, and risks may be limited to the training set and biased (Luccioni et al. 2024), potentially overlooking important aspects. Enhancements could include fine-tuning (Hu et al. 2023) or augmenting with specialized datasets (e.g., from AI Incident Database (McGregor 2021)). Second, there is a risk of incorrect outputs due to LLM hallucinations (Mittelstadt, Wachter, and Russell 2023). *UsesGen* identified 6% unrealistic uses, which were removed. Future research could explore combining classifiers and manual checks to ensure accuracy (Mittelstadt, Wachter, and Russell 2023). Third, LLMs may be overly conservative, missing risky edge-case uses due to built-in guardrails. Last, presenting LLM outputs to users could create a false sense of security (Pataranutaporn et al. 2023). Ongoing research in human-AI interaction offers strategies to mitigate these issues, such as designing cognitive forcing functions (Buçinca, Malaya, and Gajos 2021) and skill improvement (Buçinca et al. 2024).

Difficulty of Risk Classification. We focused on labeling prohibited and high-risk uses, with the remainder classified as limited or low risk. However, the EU AI Act includes an additional classification label, transparency risk, which we omitted due to the task’s inherent complexity arising from ambiguities in the Act’s wording (Veale and Zuiderveen Borgesius 2021). These ambiguities, resulting from the interplay between technical and legal jargon, pose challenges even for professionals in the field, as reflected in the moderate inter-rater agreement among our user study participants. Additionally, while the five risk categories aid in classification, practical variations in each use ultimately determine their final classification.

Generalizability. While we evaluated our framework with 25 AI practitioners on the case of FRA technology, future work should explore its applicability to other technologies and involve a larger set of AI practitioners, researchers, and the general public.

References

- Abbas Helmi, R. A.; Salsabil bin Eddy Yusuf, S.; Jamal, A.; and Bin Abdullah, M. I. 2019. Face Recognition Automatic Class Attendance System (FRACAS). In *2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, 50–55.
- Aini, Q.; Febriani, W.; Lukita, C.; Kosasi, S.; and Rahardja, U. 2022. New Normal Regulation with Face Recognition Technology Using AttendX for Student Attendance Algorithm. In *2022 International Conference on Science and Technology (ICOSTECH)*, 1–7.
- Anggraini, N.; Rozy, N. F.; and Lazuardy, R. A. 2016. Facial Recognition System for Fatigue Detection Using Intel Realsense Technology. In *2016 6th International Conference on Information and Communication Technology for The Muslim World (ICT4M)*, 248–253.
- Angin, J. T. K. P.; Johan; Sukiman; Sugianto; Simarmata, B. R.; and Suharjito. 2020. Face Recognition Application with the Complete Kernel Fisher Discriminant (CKFD) Method. In *2020 3rd International Conference on Mechanical, Electronics, Computer, and Industrial Technology (MECnIT)*, 359–364.
- Anufriiev, P.; Bashkov, Y.; and Khoma, D. 2022. Experimental Face Recognition System Based On Improved Artificial Intelligence Model. In *2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT)*, 181–186.
- Arachchilage, S. W.; and Izquierdo, E. 2019. A Framework for Real-Time Face-Recognition. In *2019 IEEE Visual Communications and Image Processing (VCIP)*, 1–4.
- Arksey, H.; and O'Malley, L. 2005. Scoping studies: Towards a methodological framework. *International Journal of Social Research Methodology: Theory and Practice*, 8: 19–32.
- Ashurst, C.; Hine, E.; Sedille, P.; and Carlier, A. 2022. Ai ethics statements: analysis and lessons learnt from neurips broader impact statements. In *Proceedings of the 2022 ACM conference on fairness, accountability, and transparency*, 2047–2056.
- Ayub, A. M.; Kolandaisamy, R.; and Hooi, K. K. 2023. Getting Smarter with Fatrix: A Facial Recognition Access Control System. In *2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)*, 149–153.
- Baltanas, S.-F.; Ruiz-Sarmiento, J.-R.; and Gonzalez-Jimenez, J. 2020. A Face Recognition System for Assistive Robots. In *Proceedings of the 3rd International Conference on Applications of Intelligent Systems*, APPIS 2020. New York, NY, USA: Association for Computing Machinery. ISBN 9781450376303.
- Banerjee, D.; and Yu, K. 2018. Robotic Arm-Based Face Recognition Software Test Automation. *IEEE Access*, 6: 37858–37868.
- Baran, R.; Rudzinski, F.; and Zeja, A. 2016. Face Recognition for Movie Character and Actor Discrimination Based on Similarity Scores. In *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, 1333–1338.
- Baykara, M.; and Daş, R. 2013. Real time face recognition and tracking system. In *2013 International Conference on Electronics, Computer and Computation (ICECCO)*, 159–163.
- Blanco Muñoz, C. M.; Gómez Cruz, F.; and Jimenez Valero, J. S. 2020. Software architecture for the application of facial recognition techniques through IoT devices. In *2020 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI)*, 1–5.
- Borboni, A.; Marinoni, P.; Nuzzi, C.; Faglia, R.; Pagani, R.; and Panada, S. 2021. Towards safe collaborative interaction empowered by face recognition. In *2021 24th International Conference on Mechatronics Technology (ICMT)*, 1–4.
- Borenstein, J.; and Howard, A. 2021. Emerging challenges in AI and the need for AI ethics education. *AI and Ethics*, 1: 61–65.
- Bouschery, S. G.; Blazevic, V.; and Piller, F. T. 2024. Artificial Intelligence-Augmented Brainstorming: How Humans and AI Beat Humans Alone. Available at SSRN 4724068.
- Braun, V.; and Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2): 77–101.
- Brown, T.; Mann, B.; Ryder, N.; Subbiah, M.; Kaplan, J. D.; Dhariwal, P.; Neelakantan, A.; Shyam, P.; Sastry, G.; Askell, A.; et al. 2020. Language models are few-shot learners. *Advances in neural information processing systems*, 33: 1877–1901.
- Buçinca, Z.; Malaya, M. B.; and Gajos, K. Z. 2021. To trust or to think: cognitive forcing functions can reduce overreliance on AI in AI-assisted decision-making. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1): 1–21.
- Buçinca, Z.; Pham, C. M.; Jakesch, M.; Ribeiro, M. T.; Olteanu, A.; and Amershi, S. 2023. Aha!: Facilitating ai impact assessment by generating examples of harms. *arXiv preprint arXiv:2306.03280*.
- Buçinca, Z.; Swaroop, S.; Paluch, A. E.; Murphy, S. A.; and Gajos, K. Z. 2024. Towards Optimizing Human-Centric Objectives in AI-Assisted Decision-Making With Offline Reinforcement Learning. *arXiv preprint arXiv:2403.05911*.
- Byun, C.; Vasicek, P.; and Seppi, K. 2023. Dispensing with Humans in Human-Computer Interaction Research. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–26.
- Calvo, R. A.; Peters, D.; and Cave, S. 2020. Advancing impact assessment for intelligent systems. *Nature Machine Intelligence*, 2(2): 89–91.
- Celine, J.; and A, S. A. 2019. Face Recognition in CCTV Systems. In *2019 International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 111–116.
- Chandolika, N.; Bhange, V.; Hedau, A.; Gaikwad, U.; Baviskar, R.; and Ahmed, A. 2023. Real-time Surveillance

- system using Face Recognition and AR. In *2023 5th Biennial International Conference on Nascent Technologies in Engineering (ICNTE)*, 1–5.
- Chilson, N. A.; and Barkley, T. D. 2021. The Two Faces of Facial Recognition Technology. *IEEE Technology and Society Magazine*, 40(4): 87–100.
- Cui, J.; Li, Z.; Yan, Y.; Chen, B.; and Yuan, L. 2023. Chatlaw: Open-source legal large language model with integrated external knowledge bases. *arXiv preprint arXiv:2306.16092*.
- Dale, J.; and Clark, A. 2018. An Ensemble of Face Recognition Algorithms for Unsupervised Expansion of Training Data. In *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, 342–347.
- Darbha, P. S.; Conti, M.; Losiouk, E.; and Maiti, R. R. 2022. Face Recognition Systems: Are you sure they only consider your face? In *2022 IEEE Security and Privacy Workshops (SPW)*, 258–264.
- Davenport, T.; and Kalakota, R. 2019. The potential for artificial intelligence in healthcare. *Future healthcare journal*, 6(2): 94.
- Dignum, V. 2019. *Responsible artificial intelligence: how to develop and use AI in a responsible way*, volume 2156. Springer.
- Dowling, M.; and Lucey, B. 2023. ChatGPT for (finance) research: The Bananarama conjecture. *Finance Research Letters*, 53: 103662.
- Drozdzowski, P.; Fischer, D.; Rathgeb, C.; Geissler, J.; Knechtlik, J.; and Busch, C. 2020. Can Generative Colourisation Help Face Recognition? In *2020 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 1–5.
- Duncan, J. A.; Kalka, N. D.; Maze, B.; and Jain, A. K. 2019. End-to-End Protocols and Performance Metrics For Unconstrained Face Recognition. In *2019 International Conference on Biometrics (ICB)*, 1–8.
- Ekambaranathan, A.; Zhao, J.; and Van Kleek, M. 2021. “Money Makes the World Go Around”: Identifying Barriers to Better Privacy in Children’s Apps From Developers’ Perspectives. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI ’21. New York, NY, USA: Association for Computing Machinery. ISBN 9781450380966.
- Ekladios, G.; Lemoine, H.; Granger, E.; Kamali, K.; and Moudache, S. 2020. Dual-Triplet Metric Learning for Unsupervised Domain Adaptation in Video Face Recognition. In *2020 International Joint Conference on Neural Networks (IJCNN)*, 1–9.
- Enegi, I. L.; Hamada, M.; and Adeshina, S. A. 2017. Adaptive multimedia learning framework with facial recognition system. In *2017 13th International Conference on Electronics, Computer and Computation (ICECCO)*, 1–6.
- European Commission. 2024. Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.
- Faizabadi, A. R.; Zaki, H. F. B. M.; Abidin, Z. B. Z.; Hashim, N. N. W. N.; and Husman, M. A. B. 2022. Efficient Region of Interest Based Metric Learning for Effective Open World Deep Face Recognition Applications. *IEEE Access*, 10: 76168–76184.
- Gavriell, B.; Fauzan, F.; Ardian, N.; and Suryaningrum, K. M. 2021. Implementation of Face Recognition Method for Attendance in Class. In *2021 1st International Conference on Computer Science and Artificial Intelligence (ICC-SAI)*, volume 1, 148–153.
- Gebbru, T.; Morgenstern, J.; Vecchione, B.; Vaughan, J. W.; Wallach, H.; Iii, H. D.; and Crawford, K. 2021. Datasheets for datasets. *Communications of the ACM*, 64(12): 86–92.
- George, A.; Mohammadi, A.; and Marcel, S. 2023. Prepended Domain Transformer: Heterogeneous Face Recognition Without Bells and Whistles. *IEEE Transactions on Information Forensics and Security*, 18: 133–146.
- Gies, W.; Overby, J.; Saraceno, N.; Frome, J.; York, E.; and Salman, A. 2020. Restricting Data Sharing and Collection of Facial Recognition Data by the Consent of the User: A Systems Analysis. In *2020 Systems and Information Engineering Design Symposium (SIEDS)*, 1–6.
- Gilardi, F.; Alizadeh, M.; and Kubli, M. 2023. ChatGPT outperforms crowd-workers for text-annotation tasks. *Proceedings of the National Academy of Sciences 120 (30)*.
- Giray, L. 2023. Prompt Engineering with ChatGPT: A Guide for Academic Writers. *Annals of Biomedical Engineering*, 1–5.
- Golden, S. D.; McLeroy, K. R.; Green, L. W.; Earp, J. A. L.; and Lieberman, L. D. 2015. Upending the Social Ecological Model to Guide Health Promotion Efforts Toward Policy and Environmental Change. *Health Education & Behavior*, 42(1_suppl): 8S–14S. PMID: 25829123.
- Golpayegani, D.; Pandit, H. J.; and Lewis, D. 2023. To Be High-Risk, or Not To Be—Semantic Specifications and Implications of the AI Act’s High-Risk AI Applications and Harmonised Standards. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, FAccT ’23*, 905–915. New York, NY, USA: ACM.
- Goodell, J. W.; Kumar, S.; Lim, W. M.; and Pattnaik, D. 2021. Artificial intelligence and machine learning in finance: Identifying foundations, themes, and research clusters from bibliometric analysis. *Journal of Behavioral and Experimental Finance*, 32: 100577.
- Gupta, S.; Maurya, A.; and Agrawal, A. K. 2022. Unconstrained Face Recognition System using Deep Neural Network: A Review. In *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, 961–966.
- Gupta, T.; and Sundareson, P. 2015. Face recognition accuracy enhancement in Consumer devices. In *2015 Third International Conference on Image Information Processing (ICIIP)*, 419–421.
- Han, X. 2022. Research on the Impact of Artificial Intelligence Assist Technology on Health Using Online Service System and Computer Facial Recognition. In *2021 3rd*

- International Conference on Artificial Intelligence and Advanced Manufacture*, AIAM2021, 2175–2180. New York, NY, USA: Association for Computing Machinery. ISBN 9781450385046.
- Hassel, A.; and Özkiziltan, D. 2023. Governing the work-related risks of AI: implications for the German government and trade unions. *Transfer: European Review of Labour and Research*, 29(1): 71–86.
- Holm, J. E.; Vermaak, N.; and Jordaan, P. W. 2019. Evaluation of a Facial Recognition Engines for a Surveillance System. In *2019 IEEE AFRICON*, 1–7.
- Hu, X.; Liao, Q.; and Peng, S. 2015. Video surveillance face recognition by more virtual training samples based on 3D modeling. In *2015 11th International Conference on Natural Computation (ICNC)*, 113–117.
- Hu, Z.; Lan, Y.; Wang, L.; Xu, W.; Lim, E.-P.; Lee, R. K.-W.; Bing, L.; and Poria, S. 2023. Llm-adapters: An adapter family for parameter-efficient fine-tuning of large language models. *arXiv preprint arXiv:2304.01933*.
- Hupont, I.; Tolan, S.; Gunes, H.; and Gómez, E. 2022. The landscape of facial processing applications in the context of the European AI Act and the development of trustworthy systems. *Scientific Reports*, 12(1): 10688.
- Hutson, M. 2023. CONFLICTING VISIONS FOR AI REGULATION. *Nature*, 620(260).
- Indra, E.; Yasir, M.; Andrian, A.; Sitanggang, D.; Sihombing, O.; Tamba, S. P.; and Sagala, E. 2020. Design and Implementation of Student Attendance System Based on Face Recognition by Haar-Like Features Methods. In *2020 3rd International Conference on Mechanical, Electronics, Computer, and Industrial Technology (MECnIT)*, 336–342.
- Ismail, S.; and Ismail, S. 2022. A Preliminary Study of Cashless Payment Face Recognition System Development in Malaysia. In *2022 16th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, 1–5.
- Kalra, I.; Singh, M.; Nagpal, S.; Singh, R.; Vatsa, M.; and Sujit, P. B. 2019. DroneSURF: Benchmark Dataset for Drone-based Face Recognition. In *2019 14th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2019)*, 1–7.
- Kanna, R. K.; Surendhar, P. A.; Rubi, J.; Jyothi, G.; Ambikapathy, A.; and Vasuki, R. 2022. Human Computer Interface Application for Emotion Detection Using Facial Recognition. In *2022 IEEE International Conference on Current Development in Engineering and Technology (CCET)*, 1–7.
- Kennedy, O.; Chiamaka, A.-O.; Princess, O. I.; and Julius-Olatunji, O. 2022. Implementation of an Embedded Masked Face Recognition System using Huskylens System-On-Chip Module. In *2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON)*, 1–7.
- Kidd, C.; and Birhane, A. 2023. How AI can distort human beliefs. *Science*, 380(6651): 1222–1223.
- Kocacinar, B.; Tas, B.; Akbulut, F. P.; Catal, C.; and Mishra, D. 2022. A Real-Time CNN-Based Lightweight Mobile Masked Face Recognition System. *IEEE Access*, 10: 63496–63507.
- Kurze, M.; and Roselius, A. 2011. Smart Glasses Linking Real Live and Social Network’s Contacts by Face Recognition. In *Proceedings of the 2nd Augmented Human International Conference*, AH ’11. New York, NY, USA: Association for Computing Machinery. ISBN 9781450304269.
- Kussul, E.; and Baydyk, T. 2015. Face recognition using special neural networks. In *2015 International Joint Conference on Neural Networks (IJCNN)*, 1–7.
- Lee, M.; Liang, P.; and Yang, Q. 2022. CoAuthor: Designing a Human-AI Collaborative Writing Dataset for Exploring Language Model Capabilities. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI ’22. New York, NY, USA: Association for Computing Machinery. ISBN 9781450391573.
- Li, B.; Qi, P.; Liu, B.; Di, S.; Liu, J.; Pei, J.; Yi, J.; and Zhou, B. 2023. Trustworthy AI: From principles to practices. *ACM Computing Surveys*, 55(9): 1–46.
- Li, P.; Prieto, L.; Mery, D.; and Flynn, P. J. 2019. On Low-Resolution Face Recognition in the Wild: Comparisons and New Techniques. *IEEE Transactions on Information Forensics and Security*, 14(8): 2000–2012.
- Liang, W.; Rajani, N.; Yang, X.; Ozoani, E.; Wu, E.; Chen, Y.; Smith, D. S.; and Zou, J. 2024. What’s documented in AI? Systematic Analysis of 32K AI Model Cards. *arXiv preprint arXiv:2402.05160*.
- Liu, N. F.; Lin, K.; Hewitt, J.; Paranjape, A.; Bevilacqua, M.; Petroni, F.; and Liang, P. 2024. Lost in the middle: How language models use long contexts. *Transactions of the Association for Computational Linguistics*, 12: 157–173.
- LMSYS. 2024. LMSYS Chatbot Arena Leaderboard.
- Loncar-Turukalo, T.; Zdravovski, E.; da Silva, J. M.; Chouvarda, I.; Trajkovic, V.; et al. 2019. Literature on wearable technology for connected health: scoping review of research trends, advances, and barriers. *Journal of Medical Internet research (JMIR)*, 21(9): e14017.
- Lu, Z.; and Yin, M. 2021. Human Reliance on Machine Learning Models When Performance Feedback is Limited: Heuristics and Risks. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI ’21. New York, NY, USA: Association for Computing Machinery. ISBN 9781450380966.
- Luccioni, S.; Akiki, C.; Mitchell, M.; and Jernite, Y. 2024. Stable bias: Evaluating societal representations in diffusion models. *Advances in Neural Information Processing Systems*, 36.
- Lukowicz, P.; et al. 2023. Interacting with Large Language Models: A Case Study on AI-Aided Brainstorming for Guesstimation Problems. In *HHAI 2023: Augmenting Human Intellect: Proceedings of the Second International Conference on Hybrid Human-Artificial Intelligence*, volume 368, 153. IOS Press.
- Manna, S.; Ghildiyal, S.; and Bhimani, K. 2020. Face Recognition from Video using Deep Learning. In *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, 1101–1106.

- Mantelero, A. 2022. *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI*. T.M.C. Asser Press. ISBN 9789462655317.
- Marques, O.; and Carson, J. 2016. Selfie Search: Image Retrieval and Face Recognition in IOS: [Invited Paper]. In *Proceedings of the Third International Symposium on Computer Vision and the Internet*, VisionNet'16, 48–53. New York, NY, USA: Association for Computing Machinery. ISBN 9781450343015.
- Martínez-Díaz, Y.; Méndez-Vázquez, H.; Luevano, L. S.; Nicolás-Díaz, M.; Chang, L.; and González-Mendoza, M. 2022. Towards Accurate and Lightweight Masked Face Recognition: An Experimental Evaluation. *IEEE Access*, 10: 7341–7353.
- McClurg, A. J. 2007. In the face of danger: Facial recognition and the limits of privacy law. *Harvard Law Review*, 120(7): 1870–1891.
- McDonald, N.; Schoenebeck, S.; and Forte, A. 2019. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW).
- McGregor, S. 2021. Preventing repeated real world AI failures by cataloging incidents: The AI incident database. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 35, 15458–15463.
- Mehta, R.; Satam, S.; Ansari, M.; and Samantaray, S. 2020. Real-Time Image Processing: Face Recognition based Automated Attendance System in-built with Two-Tier Authentication Method. In *2020 International Conference on Data Science and Engineering (ICDSE)*, 1–6.
- Miles, M.; and Huberman, M. 1994. *Qualitative Data Analysis: A Methods Sourcebook*. Sage.
- Mittelstadt, B.; Wachter, S.; and Russell, C. 2023. To protect science, we must use LLMs as zero-shot translators. *Nature Human Behaviour*, 7(11): 1830–1832.
- Mladenova, T.; Valova, I.; and Valov, N. 2021. Application of Facial Recognition with PCA and Raspberry Pi for Access Control to Luggage Lockers. In *2021 International Conference Automatics and Informatics (ICAI)*, 141–145.
- Mohamed, R.; Jafni, J. U.; and Rum, S. N. M. 2022. Real-Time Face Recognition System in Smart Classroom using Haar Cascade and Local Binary Pattern Model. In *2022 International Conference on Advanced Creative Networks and Intelligent Systems (ICACNIS)*, 1–6.
- Moraes, T. G.; Almeida, E. C.; and de Pereira, J. R. L. 2021. Smile, you are being identified! Risks and measures for the use of facial recognition in (semi-) public spaces. *AI and Ethics*, 1(2): 159–172.
- Mubarak Alburaiqi, M. S.; Md Johar, G.; Abbas Helmi, R. A.; and Hazim Alkawaz, M. 2021. Mobile Based Attendance System: Face Recognition and Location Detection using Machine Learning. In *2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC)*, 177–182.
- Müller, A.; Abbasi, W.; and Saracino, A. 2022. Demo: Usage Control using Controlled Privacy Aware Face Recognition. In *2022 IEEE Symposium on Computers and Communications (ISCC)*, 1–3.
- N, S.; Sundaram, B. M.; Kumar, V. N.; J, S.; and S, H. 2022. Face Recognition based Automated Remote Proctoring Platform. In *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, 1753–1760.
- Nanayakkara, P.; Hullman, J.; and Diakopoulos, N. 2021. Unpacking the expressed consequences of AI research in broader impact statements. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, 795–806.
- Nguyen, D. D.; Le, M. H.; Nguyen, X. H.; Ngo, H. T.; and Nguyen, M. S. 2022. Smart Desk in Hybrid Classroom: Automatic Attendance System based on Face Recognition using MTCNN and ARCFACE. In *2022 International Conference on Multimedia Analysis and Pattern Recognition (MAPR)*, 1–6.
- Okokpujie, K.; Noma-Osaghae, E.; John, S.; Grace, K.-A.; and Okokpujie, I. 2017. A face recognition attendance system with GSM notification. In *2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON)*, 239–244.
- OpenAI. 2023. GPT-4 Technical Report. arXiv:2303.08774.
- Otta, S. P.; Kolipara, S.; Malhotra, V. K.; Singh, A. R.; Panda, S.; and Hota, C. 2022a. Continuous Cloud User Authentication By Efficient Facial Recognition. In *2022 5th International Conference on Computational Intelligence and Networks (CINE)*, 01–06.
- Otta, S. P.; Kolipara, S.; Panda, S.; and Hota, C. 2022b. User Identification with Face Recognition : A Systematic Analysis. In *2022 3rd International Conference for Emerging Technology (INCET)*, 1–6.
- Owen, R.; and Pansera, M. 2019. *Responsible innovation and responsible research and innovation*. Edward Elgar Publishing.
- P, K.; A, S. L. T.; and R, S. 2023. Face Recognition Attendance System Using Local Binary Pattern Algorithm. In *2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (VITECoN)*, 1–6.
- Pascua, A. R. A.; Rivera, M.; Guillermo, M.; Bandala, A.; and Sybingco, E. 2022. Face Recognition and Identification Using Successive Subspace Learning for Human Resource Utilization Assessment. In *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, 1375–1380.
- Pataranutaporn, P.; Liu, R.; Finn, E.; and Maes, P. 2023. Influencing human–AI interaction by priming beliefs about AI can increase perceived trustworthiness, empathy and effectiveness. *Nature Machine Intelligence*, 5(10): 1076–1086.
- Patel, N.; Sohi, Y. S.; and Reddy, S. 2021. FaceCognize: An approach to Face Recognition for low resolution image. In *2021 Asian Conference on Innovation in Technology (ASIANCON)*, 1–8.

- Peters, M.; Godfrey, C.; Khalil, H.; Mcinerney, P.; Parker, D.; and Soares, C. 2015. Guidance for conducting systematic scoping reviews. *International Journal of Evidence-Based Healthcare*, 13(3).
- Phaal, R.; Farrukh, C. J.; and Probert, D. R. 2004. Technology roadmapping—A planning framework for evolution and revolution. *Technological forecasting and social change*, 71(1-2): 5–26.
- Pinto, N.; Stone, Z.; Zickler, T.; and Cox, D. 2011. Scaling up biologically-inspired computer vision: A case study in unconstrained face recognition on facebook. In *CVPR 2011 WORKSHOPS*, 35–42.
- Prathyusha, N.; Pooja, P.; and Vijay Vasanth, A. 2023. Blockchain based E-Voting system with Facial Recognition. In *2023 International Conference on Inventive Computation Technologies (ICICT)*, 1203–1210.
- Praveen, G.; and Dakala, J. 2020. Face Recognition: Challenges and Issues in Smart City/Environments. In *2020 International Conference on COMMunication Systems & NETWORKS (COMSNETS)*, 791–793.
- Prunkl, C. E.; Ashurst, C.; Anderljung, M.; Webb, H.; Leike, J.; and Dafoe, A. 2021. Institutionalizing ethics in AI through broader impact requirements. *Nature Machine Intelligence*, 3(2): 104–110.
- Raghavendra, R.; Vetrekar, N.; Raja, K. B.; Gad, R. S.; and Busch, C. 2018. Detecting Disguise Attacks on Multi-spectral Face Recognition Through Spectral Signatures. In *2018 24th International Conference on Pattern Recognition (ICPR)*, 3371–3377.
- Rahman, L. A.; and Marikannan Booma, P. 2022. The Early Detection of Autism Within Children Through Facial Recognition; A Deep Transfer Learning Approach. In *2022 2nd International Conference on New Technologies of Information and Communication (NTIC)*, 1–11.
- Raj, R.; Balakrishna, S.; M.L.J, S.; Kulal, D. H.; and Singh, S. 2022. A survey on machine learning-based facial recognition algorithm. In *2022 International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN)*, 1–7.
- Raji, I. D.; Gebru, T.; Mitchell, M.; Buolamwini, J.; Lee, J.; and Denton, E. 2020. Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, AIES '20*, 145–151. New York, NY, USA: Association for Computing Machinery. ISBN 9781450371100.
- Ramachandra, R.; and Busch, C. 2017. Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey. *ACM Comput. Surv.*, 50(1).
- Rao, A. 2022. AttenFace: A Real Time Attendance System Using Face Recognition. In *2022 IEEE 6th Conference on Information and Communication Technology (CICT)*, 1–5.
- Rathgeb, C.; Dantcheva, A.; and Busch, C. 2019. Impact and Detection of Facial Beautification in Face Recognition: An Overview. *IEEE Access*, 7: 152667–152678.
- Ratnaparkhi, S. T.; Singh, P.; Tandasi, A.; and Sindhwani, N. 2021. Comparative Analysis of Classifiers for Criminal Identification System Using Face Recognition. In *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 1–6.
- Reimers, N.; and Gurevych, I. 2019. Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks. In *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP)*, 3982–3992.
- Rey, W. P.; Africano, K. I. C.; Cosca, K. I. S.; and Landayan, P. J. S. 2022. Arrest Records Management System (ARMS) Using Fingerprint and Face Recognition: A Criminal Record Management System for the City of Makati, Philippines. In *Proceedings of the 5th International Conference on Information Science and Systems, ICISS '22*, 70–76. New York, NY, USA: Association for Computing Machinery. ISBN 9781450396837.
- Rillig, M. C.; Ågerstrand, M.; Bi, M.; Gould, K. A.; and Sauerland, U. 2023. Risks and benefits of large language models for the environment. *Environmental Science & Technology*, 57(9): 3464–3466.
- Rudraraju, S. R.; Suryadevara, N. K.; and Negi, A. 2019. Face Recognition in the Fog Cluster Computing. In *2019 IEEE International Conference on Signal Processing, Information, Communication & Systems (SPICSCON)*, 45–48.
- Saldaña, J. 2015. *The Coding Manual for Qualitative Researchers*. Sage.
- Salihbašić, A.; and Orehovački, T. 2019. Development of Android Application for Gender, Age and Face Recognition Using OpenCV. In *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1635–1640.
- Sarkar, E.; Benkraouda, H.; Krishnan, G.; Gamil, H.; and Maniatakos, M. 2022. FaceHack: Attacking Facial Recognition Systems Using Malicious Facial Characteristics. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 4(3): 361–372.
- Sati, V.; Garg, D.; Choudhury, T.; and Aggarwal, A. 2018. Facial Recognition-Application and Future: A Review. In *2018 International Conference on System Modeling & Advancement in Research Trends (SMART)*, 231–235.
- Scherhag, U.; Raghavendra, R.; Raja, K. B.; Gomez-Barrero, M.; Rathgeb, C.; and Busch, C. 2017. On the vulnerability of face recognition systems towards morphed face attacks. In *2017 5th International Workshop on Biometrics and Forensics (IWBF)*, 1–6.
- Sharma, A.; Rushton, K.; Lin, I.; Wadden, D.; Lucas, K.; Miner, A.; Nguyen, T.; and Althoff, T. 2023. Cognitive Reframing of Negative Thoughts through Human-Language Model Interaction. In *ACL: Proceedings of the 61st Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*.
- Shaukat, Z.; Fang, J.; Azeem, M.; Akhtar, F.; and Ali, S. 2018. Cloud Based Face Recognition for Google Glass. In *Proceedings of the 2018 International Conference on Computing and Artificial Intelligence, ICCAI '18*, 104–111.

- New York, NY, USA: Association for Computing Machinery. ISBN 9781450364195.
- Sherman, E.; and Eisenberg, I. 2024. AI Risk Profiles: A Standards Proposal for Pre-deployment AI Risk Disclosures. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 38, 23047–23052.
- Shieh, J. 2023. Best practices for prompt engineering with OpenAI API.
- Singh, A.; Mishra, S.; Sharma, P.; Singh, V.; and Arya, A. 2023. Facial Recognition for Crime Control: A Machine Learning-based Solution. In *2023 4th International Conference on Intelligent Engineering and Management (ICIEM)*, 1–6.
- Singh, G.; Gupta, I.; Singh, J.; and Kaur, N. 2022. Face Recognition using Open Source Computer Vision Library (OpenCV) with Python. In *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 1–6.
- Smith, D. F.; Wiliem, A.; and Lovell, B. C. 2015a. Binary watermarks: a practical method to address face recognition replay attacks on consumer mobile devices. In *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015)*, 1–6.
- Smith, D. F.; Wiliem, A.; and Lovell, B. C. 2015b. Face Recognition on Consumer Devices: Reflections on Replay Attacks. *IEEE Transactions on Information Forensics and Security*, 10(4): 736–745.
- Smuha, N. A. 2021. From a ‘race to AI’ to a ‘race to AI regulation’: regulatory competition for artificial intelligence. *Law, Innovation and Technology*, 13(1): 57–84.
- Spijkerman, R.; and Ehlers, E. 2022. Proposed Face Recognition System Based on Immune Inspired Anomaly Detection Using Symbiotic Agents. In *Proceedings of the 2021 4th International Conference on Computational Intelligence and Intelligent Systems, CIIS '21*, 19–24. New York, NY, USA: Association for Computing Machinery. ISBN 9781450385930.
- Sraml Gonzalez, J.; and Gulbrandsen, M. 2022. Innovation in established industries undergoing digital transformation: the role of collective identity and public values. *Innovation*, 24(1): 201–230.
- Srinivas, N.; Ricanek, K.; Michalski, D.; Bolme, D. S.; and King, M. 2019. Face Recognition Algorithm Bias: Performance Differences on Images of Children and Adults. In *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2269–2277.
- Stahl, B. C.; Antoniou, J.; Bhalla, N.; Brooks, L.; Jansen, P.; Lindqvist, B.; Kirichenko, A.; Marchal, S.; Rodrigues, R.; Santiago, N.; et al. 2023. A systematic review of artificial intelligence impact assessments. *Artificial Intelligence Review*, 56(11): 12799–12831.
- Stark, L. 2019. Facial Recognition is the Plutonium of AI. *XRDS*, 25(3): 50–55.
- Tahaei, M.; Constantinides, M.; Quercia, D.; Kennedy, S.; Muller, M.; Stumpf, S.; Liao, Q. V.; Baeza-Yates, R.; Aroyo, L.; Holbrook, J.; et al. 2023. Human-Centered Responsible Artificial Intelligence: Current & Future Trends. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–4.
- Tanadi, R.; and Yusuf, R. 2020. Face Recognition Implementation on Public Spaces Usability and Performance Review. In *2020 6th International Conference on Interactive Digital Media (ICIDM)*, 1–5.
- Tapyou, K.; Chaisil, P.; and Muangprathub, J. 2021. Smart School Attendance System using Face Recognition with Near Optimal Imaging. In *2021 18th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, 1–5.
- Tariq, S.; Jeon, S.; and Woo, S. S. 2022. Am I a Real or Fake Celebrity? Evaluating Face Recognition and Verification APIs under Deepfake Impersonation Attack. In *Proceedings of the ACM Web Conference 2022, WWW '22*, 512–523. New York, NY, USA: Association for Computing Machinery. ISBN 9781450390965.
- Tariq, S.; Jeon, S.; and Woo, S. S. 2023. Evaluating Trustworthiness and Racial Bias in Face Recognition APIs Using Deepfakes. *Computer*, 56(5): 51–61.
- Teleron, J. I.; Galleros, D. B.; and Reyna, R. A. 2022. Implementation of Student Monitoring Through Face Recognition and Temperature Using Raspberry Pi. In *2022 2nd International Conference in Information and Computing Research (iCORE)*, 36–42.
- Trianti, C. A.; Kristianto, B.; and Hendry. 2021. Integration of Flask and Python on The Face Recognition Based Attendance System. In *2021 2nd International Conference on Innovative and Creative Information Technology (ICITech)*, 164–168.
- Varkarakis, V.; and Corcoran, P. 2020. Dataset Cleaning — A Cross Validation Methodology for Large Facial Datasets using Face Recognition. In *2020 Twelfth International Conference on Quality of Multimedia Experience (QoMEX)*, 1–6.
- Veale, M.; and Zuiderveen Borgesius, F. 2021. Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, 22(4): 97–112.
- Verma, V. K.; Kansal, V.; and Bhatnagar, P. 2020. Patient Identification using Facial Recognition. In *2020 International Conference on Futuristic Technologies in Control Systems & Renewable Energy (ICFCR)*, 1–7.
- Vetrekar, N.; Raghavendra, R.; Raja, K. B.; Gad, R. S.; and Busch, C. 2020. Disguise Face Recognition Based On Spectral Imaging. In *Proceedings of the 11th Indian Conference on Computer Vision, Graphics and Image Processing, ICVGIP '18*. New York, NY, USA: Association for Computing Machinery. ISBN 9781450366151.
- Wang, H.; and Zhao, L. 2010. A Face Recognition Method Based on DiaPCA and Neural Network. In *2010 International Conference on Electrical and Control Engineering*, 53–56.

Wang, P.; Lin, W.-H.; Wu, B.-H.; Chao, K.-M.; and Lo, C.-C. 2018. A Cross-Age Face Recognition Approach Using Fog Computing Architecture for User Authentication on Mobile Devices. In *2018 IEEE 15th International Conference on e-Business Engineering (ICEBE)*, 86–93.

Wang, Q.; Madaio, M.; Kane, S.; Kapania, S.; Terry, M.; and Wilcox, L. 2023. Designing responsible ai: Adaptations of ux practice to meet responsible ai challenges. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–16.

Wang, Z. J.; Kulkarni, C.; Wilcox, L.; Terry, M.; and Madaio, M. 2024. Farsight: Fostering Responsible AI Awareness During AI Application Prototyping. *arXiv preprint arXiv:2402.15350*.

Wei, J.; Wang, X.; Schuurmans, D.; Bosma, M.; ichter, b.; Xia, F.; Chi, E.; Le, Q. V.; and Zhou, D. 2022. Chain-of-Thought Prompting Elicits Reasoning in Large Language Models. In Koyejo, S.; Mohamed, S.; Agarwal, A.; Belgrave, D.; Cho, K.; and Oh, A., eds., *Advances in Neural Information Processing Systems*, volume 35, 24824–24837. Curran Associates, Inc.

Weidinger, L.; Rauh, M.; Marchal, N.; Manzini, A.; Hendricks, L. A.; Mateos-Garcia, J.; Bergman, S.; Kay, J.; Griffin, C.; Bariach, B.; et al. 2023. Sociotechnical safety evaluation of generative ai systems. *arXiv preprint arXiv:2310.11986*.

Wu, T.; Terry, M.; and Cai, C. J. 2022. AI Chains: Transparent and Controllable Human-AI Interaction by Chaining Large Language Model Prompts. CHI '22. New York, NY, USA: Association for Computing Machinery. ISBN 9781450391573.

Yang, X.; Liang, W.; and Zou, J. 2024. Navigating Dataset Documentations in AI: A Large-Scale Analysis of Dataset Cards on HuggingFace. In *The Twelfth International Conference on Learning Representations (ICLR)*.

Zhang, S.; Feng, Y.; and Sadeh, N. 2021. Facial recognition: Understanding privacy concerns and attitudes across increasingly diverse deployment scenarios. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, 243–262.

Zhao, Y.; Wu, S.; Reynolds, L.; and Azenkot, S. 2018. A Face Recognition Application for People with Visual Impairments: Understanding Use Beyond the Lab. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, 1–14. New York, NY, USA: Association for Computing Machinery. ISBN 9781450356206.

Zheng, Z.; Chen, K.-Y.; Cao, X.-Y.; Lu, X.-Z.; and Lin, J.-R. 2023. Llm-funcmapper: Function identification for interpreting complex clauses in building codes via llm. *arXiv preprint arXiv:2308.08728*.

Zhou, X.; and Keoh, S. L. 2020. Deployment of Facial Recognition Models at the Edge: A Feasibility Study. In *2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 214–219.

Appendix

(A) UsesGen

Table 2: We identified a list of 46 domains from the EU AI Act (European Commission 2024) and an interactive session with our research team ($N=8$). Among these, 40 domains are from the EU AI Act, and 6 additional domains – not covered by the previous list of 40 domains – were identified during the session with our team (indicated by an asterisk *).

No.	Domain	No.	Domain
1	Biometric identification and categorization of natural persons	24	Democracy
2	Family	25	Media and Communication
3	Romantic relationships and friendships	26	Accessibility and Inclusion
4	Health and Healthcare	27	Energy
5	Well-being	28	Military and Defense
6	Human-Computer Interaction	29	Administration of justice and democratic processes
7	Finance and Investment	30	Government Services and Administration
8	Education and vocational training	31	Diplomacy and Foreign Policy
9	Employment, workers management and access to self-employment	32	Food Safety and Regulation
10	Essential private services and public services and benefits	33	Crisis Management and Emergency Response
11	Recommender Systems and Personalization	34	Humanitarian Aid
12	Social Media	35	Transport and Logistics
13	Sports and Recreation	36	Urban Planning
14	Arts and Entertainment	37	Counterterrorism
15	Security and Cybersecurity	38	Environment and Sustainability
16	Marketing and Advertising	39	International Law Enforcement and Cooperation
17	Agriculture and Farming	40	Climate Change Mitigation and Adaptation
18	Entrepreneurship	41	Gaming and interactive experiences*
19	Autonomous Robots and Robotics	42	Hobbies*
20	Innovation and Research	43	Smart home*
21	Management and Operation of critical infrastructure	44	Social and Community Services*
22	Law enforcement	45	Public and private transportation*
23	Migration, Asylum and Border control management	46	Interpersonal Communication*

(B) GT: FRA Uses from the Literature

1. Access control for buildings, areas, storage places, banks' vaults and lockers. (Scherhag et al. 2017; Okokpujie et al. 2017; Baykara and Daş 2013; Manna, Ghildiyal, and Bhimani 2020; Hu, Liao, and Peng 2015; Kussul and Baydyk 2015; Sati et al. 2018; Tanadi and Yusuf 2020; Blanco Muñoz, Gómez Cruz, and Jimenez Valero 2020; Ismail and Ismail 2022; Mladenova, Valova, and Valov 2021; Borboni et al. 2021; Angin et al. 2020; Gavriell et al. 2021; Müller, Abbasi, and Saracino 2022; Ayub, Kolandaisamy, and Hooi 2023; Teleron, Galleros, and Reyna 2022; Anufriiev, Bashkov, and Khoma 2022; Patel, Sohi, and Reddy 2021; Kocacinar et al. 2022; Martínez-Díaz et al. 2022; Raj et al. 2022; Otta et al. 2022b; Kennedy et al. 2022; Kanna et al. 2022; Dale and Clark 2018; Otta et al. 2022a; Zhou and Keoh 2020; Holm, Vermaak, and Jordaan 2019; George, Mohammadi, and Marcel 2023; Ramachandra and Busch 2017; Spijkerman and Ehlers 2022)
2. Access control for technology, secure networks, and resources. (Singh et al. 2022; Müller, Abbasi, and Saracino 2022; Ramachandra and Busch 2017)
3. Detect unauthorized personnel. (Zhou and Keoh 2020)
4. Securely register and manage visitors. (Zhou and Keoh 2020; P, A, and R 2023)
5. Provide real-time information about visitors in high-profile buildings. (Chandollikar et al. 2023)
6. Identify men in female-reserved coaches or women-only areas. (Praveen and Dakala 2020)
7. Visualize building occupancy and peak hours and determine foot traffic patterns. (Pascua et al. 2022)
8. Identify individuals approaching homes for example through smart doorbells. (Praveen and Dakala 2020; Chilson and Barkley 2021)
9. Trigger an alarm when unidentified individuals enter a home. (Sati et al. 2018)
10. Enable unlocking devices and apps. (Scherhag et al. 2017; Okokpujie et al. 2017; Baykara and Daş 2013; Ratnaparkhi et al. 2021; Sati et al. 2018; Singh et al. 2022; Mladenova, Valova, and Valov 2021; Singh et al. 2023; Anufriiev, Bashkov, and Khoma 2022; Darbha et al. 2022; Chilson and Barkley 2021; Smith, Wiliem, and Lovell 2015b; Banerjee and Yu 2018; Smith, Wiliem, and Lovell 2015a; Ekladious et al. 2020; Wang et al. 2018; Mubarak Alburaiqi et al. 2021; Zhou and Keoh 2020; Gupta, Maurya, and Agrawal 2022)
11. Enable unlocking cars and driving them. (Okokpujie et al. 2017; Gupta and Sundareson 2015; Raj et al. 2022)
12. Notify owners if someone attempts to steal their car. (Okokpujie et al. 2017)

(E) System role

(A) Instructions

- (1) Create list
- (2) Request number of uses
- (3) Request action verbs
- (4) Use consistent specificity

(B) Risk concepts

(A) Instructions

- (5) Use non-expert language
- (6) Avoid duplicates
- (7) Use precise language

(C) Domains

(A) Instructions

- (1) Categorize uses
- (2) Justification
- (3) Consider FRT

(B) Definitions

of the three categories of being realistic

(D) Examples

```
messages = [
  {
    'role': 'system',
    'content': "" As a Senior Facial Recognition Technology Specialist, you are an expert dedicated to staying at the forefront of advancements in facial recognition technology. In this pivotal role, you are entrusted with reviewing, and cataloging the diverse applications and use cases of facial recognition technology across multiple domains.""
  },

```

```
{
  'role': 'user',
  'content': "" Create a comprehensive and self-explanatory list, in JSON format, detailing the various uses of facial recognition technology. Each dictionary in the created list describes a particular use case or application of facial recognition technology.
  Provide three uses for each of the 8 domains listed below.
  The uses must contain specific details about how the technology is used, by using action verbs that clearly describe the actions, activities, or processes of the uses.
  The level of specificity should be consistent across all uses.

```

For each of these uses, you must output the following 6 elements each in less than 7 words:

- (1) Use: An element of a series of numbered uses, starting with 1. Each use should be listed consecutively.
- (2) Domain: The domain that represents the area or sector the AI system is intended to be used in.
- (3) Purpose: The purpose or objective that is intended to be accomplished by using an AI system.
- (4) Capability: The capability of the AI system that enables the realization of its purpose and reflects the technological capability.
- (5) AI user: The entity or individual in charge of deploying and managing the AI system, including individuals, organizations, corporations, public authorities, and agencies responsible for its operation and management.
- (6) AI subject: The individual directly affected by the use of the AI system, experiencing its effects and consequences. They interact with or are impacted by the AI system's processes, decisions, or outcomes.

Ensure that each concept is specific and easy to understand for non-experts. Avoid duplicate purposes or objectives. and use clear and precise language to describe the uses' concepts.

- Domains to be included are the following:
1. Employment, workers management and access to self-employment
 2. Essential private services and public services and benefits
 3. Recommender Systems and Personalization
 4. Social Media
 5. Sports and Recreation
 6. Arts and Entertainment
 7. Security and Cybersecurity
 8. Marketing and Advertising

Categorize each of these uses into three specific categories: Already existent, Upcoming, and Unlikely uses. Provide a one-sentence justification for each categorization. Keep in mind that any applications should be assessed considering their implementation through facial recognition technology.

- Take account of the following definitions of the three categories when categorizing the uses of AI technology:
1. Already existent uses of facial recognition technology: encompass uses that are currently implemented and well-established uses.
 2. Upcoming uses of facial recognition technology: encompass uses that are currently under development, being researched, or subject to discussions. So far, these uses have either not been implemented or have been severely limited in practice due to various reasons.
 3. Unlikely uses of facial recognition technology encompass: uses that lack value, usability, applicability, or practicality, or are deemed unnecessary, impossible, incoherent, or unrealistic.

```
Follow this example structure for reporting the identified uses:
[ ...
  {
    "Use": 2,
    "Domain": "Finance and Investment",
    "Purpose": "Fraud detection and prevention",
    "Capability": "Verifying customer identity for transactions",
    "AI User": "Banks, financial institutions",
    "AI Subject": "Customers"
    "Realism Label": "Already existent",
    "Realism Label Justification": "This method has been adopted by financial institutions worldwide, reflecting a growing trend towards biometric security measures in the banking sector.",
  }, ...
]
""
]
```

```
response = get_completion_from_messages(messages)
print(response)
```

maximum output token length = 7000

Figure 4: **UsesGen**. The prompt generates a list of uses for a given AI technology, e.g., FRA. These LLM-generated uses are required to be outputted in the format of 5 risk concepts (domain, purpose, capability, AI user, AI subject) (Golpayegani, Pandit, and Lewis 2023). This format allows the subsequent RiskLabelling prompt to evaluate the risk of a given AI technology use. To identify the most comprehensive and realistic list of LLM-generated uses, we examined different UsesGen configurations. These prompt configurations included the model temperature, number of requested uses per domain (2 or 3), and prompt elements (Variation 1-3). Variation 1 of UsesGen encompassed an instruction (A), definitions of risk concepts and the three categories of being realistic (B), and domains (C), that correspond to the necessary elements (Figure ??). In Variation 2, we introduced the system role (D), while in Variation 3, we included an additional five examples (E).

13. Track worker and student attendance. (Scherhag et al. 2017; Okokpujie et al. 2017; Abbas Helmi et al. 2019; Indra et al. 2020; Aini et al. 2022; Celine and A 2019; Ratnaparkhi et al. 2021; Trianti, Kristianto, and Hendry 2021; Singh et al. 2022; Tanadi and Yusuf 2020; Ismail and Ismail 2022; Tapyou, Chaisil, and Muangprathub 2021; Angin et al. 2020; Singh et al. 2023; Gavriell et al. 2021; Teleron, Galleros, and Reyna 2022; Rao 2022; Patel, Sohi, and Reddy 2021; Kocacinar et al. 2022; Martínez-Díaz et al. 2022; Mubarak Alburaiqi et al. 2021; Pascua et al. 2022; Mehta et al. 2020; Zhou and Keoh 2020; P, A, and R 2023; Mohamed, Jafni, and Rum 2022; Nguyen et al. 2022)
14. Check if students and workers comply with regulations. (Singh et al. 2022; P, A, and R 2023)
15. Monitor and track students' activities and performance to aid university examinations. (Singh et al. 2023; N et al. 2022; P, A, and R 2023)
16. Identify demographic attributes of individuals, including gender, age, ethnicity, and sexual orientation. (Salihbašić and Orehovački 2019; Manna, Ghildiyal, and Bhimani 2020; Praveen and Dakala 2020; Singh et al. 2022; Drozdowski et al. 2020; Raji et al. 2020)
17. Perform profiling to identify patterns and characteristics of individuals or groups. (Borboni et al. 2021)
18. Implement targeted recognition systems that customize responses or services based on a person's ethnicity or gender. (Chilson and Barkley 2021)
19. Customize advertisements and promotions for targeted marketing. (Praveen and Dakala 2020)
20. Identify individuals' shopping habits for personalized discounts and offerings. (Chilson and Barkley 2021)
21. Evaluate consumer satisfaction. (Chilson and Barkley 2021; Raji et al. 2020)
22. Monitor wait times and moods in check-out or customer service lines. (Chilson and Barkley 2021)
23. Personalized recommendations, surroundings, and services for smart homes, automotive environments, and travel industry. (Praveen and Dakala 2020; Gupta and Sundareson 2015)
24. Identify and track criminals, suspects, stalkers, or terrorists. (Baykara and Daş 2013; Manna, Ghildiyal, and Bhimani 2020; Ratnaparkhi et al. 2021; Praveen and Dakala 2020; Angin et al. 2020; Singh et al. 2023; Gavriell et al. 2021; Patel, Sohi, and Reddy 2021; Chilson and Barkley 2021; Gies et al. 2020; Kennedy et al. 2022; Kanna et al. 2022; Zhou and Keoh 2020; Shaikat et al. 2018; Raji et al. 2020; Rey et al. 2022)
25. Recording an arrested individual's facial information. (Mehta et al. 2020; Duncan et al. 2019)
26. Gathering, analyzing, and interpreting evidence from a crime scene or incident. (Praveen and Dakala 2020; Rathgeb, Dantcheva, and Busch 2019; Mehta et al. 2020; Vetrekar et al. 2020)
27. Register traffic violations by rental transport users. (Praveen and Dakala 2020)
28. Establish a unified penalty system, collecting fines for various violations such as fare dodging. (Praveen and Dakala 2020)
29. Define groups of people and create whitelists for VIPs and blacklists for unwanted individuals. (Singh et al. 2023)
30. Compare individuals against watchlists containing names, identifiers, or attributes of known individuals of interest or potential risks. (Manna, Ghildiyal, and Bhimani 2020; Ekladios et al. 2020; Raj et al. 2022; Gupta, Maurya, and Agrawal 2022)
31. Prevent child exploitation and abduction. (Srinivas et al. 2019)
32. Search for and identify missing persons. (Ratnaparkhi et al. 2021; Praveen and Dakala 2020; Sarkar et al. 2022; Patel, Sohi, and Reddy 2021; Chilson and Barkley 2021; Gupta, Maurya, and Agrawal 2022; Spijkerman and Ehlers 2022)
33. Identify abusive law enforcement officers. (Chilson and Barkley 2021)
34. Implement face tagging in images. (Manna, Ghildiyal, and Bhimani 2020; Kussul and Baydyk 2015; Ratnaparkhi et al. 2021; Singh et al. 2023; Pinto et al. 2011; Chilson and Barkley 2021; Gies et al. 2020; Gupta, Maurya, and Agrawal 2022; Tariq, Jeon, and Woo 2023, 2022)
35. Create digital photo books. (Srinivas et al. 2019)
36. Alert individuals when photographs with their faces are posted online. (Sati et al. 2018)
37. Detect and report inappropriate pictures using facial recognition and pattern analysis. (Sarkar et al. 2022)
38. Group photos based on individuals present. (Spijkerman and Ehlers 2022)
39. Conduct face scans to search for specific individuals in pictures. (Sati et al. 2018; Marques and Carson 2016; Raji et al. 2020)
40. Use selfies to find users' doppelganger in a database of recognized paintings. (Chilson and Barkley 2021)
41. Recognize when fake profiles use someone else's face. (Chilson and Barkley 2021)
42. Offer friend suggestions on social media platforms. (Sarkar et al. 2022)
43. Prevent online dating fraud. (Sarkar et al. 2022)
44. Enable face authentication-based mobile payments and other banking services. (Praveen and Dakala 2020; Sati et al. 2018; Singh et al. 2022; Ismail and Ismail 2022; Mladenova, Valova, and Valov 2021; Borboni et al. 2021; Chilson and Barkley 2021; Martínez-Díaz et al. 2022; Smith, Wiliem, and Lovell 2015a; Raj et al. 2022; Faizabadi et al. 2022)
45. Compare a customer's face during ATM usage with database to reduce fraudulent activities. (Baykara and Daş 2013; Singh et al. 2023)
46. Payments on public transport (E.g. metro trains, public buses, toll gates). (Praveen and Dakala 2020)
47. Identify patients and facilitate check-in and other processes for patients, for example, provide notifications to respective doctors, generate e-prescriptions for patients, update recent improvements in a patient's case study. (Praveen and Dakala 2020;

- Verma, Kansal, and Bhatnagar 2020)
48. Identify healthcare staff. (Praveen and Dakala 2020; Darbha et al. 2022)
 49. Track staff and patients to keep a record of the movement and presence of both staff members and patients within a healthcare facility. (Praveen and Dakala 2020; Verma, Kansal, and Bhatnagar 2020)
 50. Streamline and manage medicine distribution in healthcare settings. (Praveen and Dakala 2020; Chilson and Barkley 2021)
 51. Diagnose or support detection of diseases in individuals. (Praveen and Dakala 2020; Mubarak Alburaiqi et al. 2021; Rahman and Marikannan Booma 2022)
 52. Retrieve critical information of people in emergencies, such as their blood group. (Praveen and Dakala 2020)
 53. Conduct real-time mental health tests. (Han 2022)
 54. Provide automatic floor selection in elevators for elderly and individuals with disabilities. (Praveen and Dakala 2020)
 55. Assist individuals with impairments by identifying their friends and people, providing reminders of names, and relevant information about them. (Ekladios et al. 2020; Pascua et al. 2022; Zhao et al. 2018; Shaukat et al. 2018)
 56. Assist individuals with visual impairments in taking photos. (Zhao et al. 2018)
 57. Initiate robot operations only when it recognizes an operator in its workspace. (Borboni et al. 2021)
 58. Enable assistive robots to recognize individuals in a home environment. (Baltanas, Ruiz-Sarmiento, and Gonzalez-Jimenez 2020)
 59. Facilitate voter identification processes. (Singh et al. 2023; Prathyusha, Pooja, and Vijay Vasanth 2023)
 60. Provide tailored learning experiences to suit individual needs. (Enegi, Hamada, and Adeshina 2017)
 61. Create multimedia content using facial recognition. (Wang and Zhao 2010; Rathgeb, Dantcheva, and Busch 2019; Varkarakis and Corcoran 2020; Gies et al. 2020)
 62. Identify and differentiate between various characters and actors in movies, making it highly beneficial for content discovery and delivery platforms that seek to provide content based on specific characters or actors. (Baran, Rudzinski, and Zeja 2016)
 63. Overlay cosmetic changes for users. (Chilson and Barkley 2021)
 64. Use photo and video filters and special beautification effects. (Chilson and Barkley 2021; Stark 2019)
 65. Streamline check-ins and boarding and reduce waiting times at airports. (Baykara and Daş 2013; Manna, Ghildiyal, and Bhimani 2020; Kussul and Baydyk 2015; Praveen and Dakala 2020; Chilson and Barkley 2021; Raj et al. 2022; Kennedy et al. 2022)
 66. Identify travelers at border crossings to automate border crossing procedures (traveler identification, biometric passport, passport-checking). (Scherhag et al. 2017; Arachchilage and Izquierdo 2019; Baykara and Daş 2013; Praveen and Dakala 2020; Tanadi and Yusuf 2020; Mladenova, Valova, and Valov 2021; Drozdowski et al. 2020; Sarkar et al. 2022; Srinivas et al. 2019; Raghavendra et al. 2018; Gupta, Maurya, and Agrawal 2022; Duncan et al. 2019; Ramachandra and Busch 2017)
 67. Verify documents, such as passports, visas, and driver's licenses. (Kussul and Baydyk 2015; Singh et al. 2023; Gupta, Maurya, and Agrawal 2022; Spijkerman and Ehlers 2022)
 68. Identify and verify people in train stations and stadiums. (Kennedy et al. 2022)
 69. Detect fatigue in individuals. (Anggraini, Rozy, and Lazuardy 2016)
 70. Detect emotions in individuals. (Kanna et al. 2022; Raji et al. 2020)
 71. Facilitate recruitment processes by informing hiring decisions and help job interviewers to view candidate's previous records. (Shaukat et al. 2018; Raji et al. 2020)
 72. Help people recognize faces by using smart glasses to display names and social network activities of identified people. (Kurze and Roselius 2011; Shaukat et al. 2018)
 73. Monitor and surveil people. (Salihbašić and Orehovački 2019; Arachchilage and Izquierdo 2019; Manna, Ghildiyal, and Bhimani 2020; Hu, Liao, and Peng 2015; Praveen and Dakala 2020; Rudraraju, Suryadevara, and Negi 2019; Tanadi and Yusuf 2020; Blanco Muñoz, Gómez Cruz, and Jimenez Valero 2020; Wang and Zhao 2010; Borboni et al. 2021; Angin et al. 2020; Li et al. 2019; Kalra et al. 2019; Ekladios et al. 2020; Kanna et al. 2022; Mubarak Alburaiqi et al. 2021; Dale and Clark 2018; Mehta et al. 2020; Holm, Vermaak, and Jordaan 2019; Raji et al. 2020)
 74. Facilitate tourists in meeting new people. (Shaukat et al. 2018)

(C) RiskLabelling

(D) List of FRA Uses Generated by UsesGen

(E) System role

(A) Instructions

- (1) Classification
- (2) Four steps
- (3) Make accurate judgments
- (4) Consider all regulations

(B) Legal documents

Relevant Section of the EU AI Act (for what is unacceptable and high-risk) and its amendments

(C) Placeholder for an LLM-generated use to be assessed along five risk concepts

(D) Output structure

```
messages = [
  {
    'role': 'system',
    'content': ""You are an experienced regulatory compliance specialists who works in the field of AI technology regulation. You are thoughtful, decisive, experienced and conscientious. You have access to the entirety of the EU AI Act and its amendments, which outline how various AI technologies are to be regulated and risk-classified within the European Union.""
  },
  {
    'role': 'user',
    'content': "Classify the following AI system by utilizing a three-tier classification: 1) Unacceptable Risk, 2) High Risk, and 3) Not Classified as High Risk or Unacceptable Risk. Follow these four steps below: 1. Write a brief description of the AI system, using similar language to the EU AI Act. The description should start with 'The AI system intended to be used ...', and be no longer than two sentences. 2. Determine whether the AI system is of Unacceptable Risk or High Risk, providing the exact text from the EU AI Act and explaining the reasoning. Be very strict and verify the reasoning. Assume High Risk unless there is clear evidence for Unacceptable Risk. Pay particular attention to the subject and user of the AI system, as this is critical for classification. Ensure that the subject and user align with the text. They are very important. Also, ensure that you understand the purpose and the capability of the AI system as this is highly critical for the risk classification. For example, the capability to verify patient identities by using AI technology implies the use of biometric identification of patients. Be aware of these and similar cases. 3. Go through all the amendments to the EU AI Act and ensure that nothing has changed that would affect the classification. If something has changed, update the classification accordingly and explicitly reference the amendment that most closely resembles the AI system. The amendments can be found under the text: 'Here are some important amendments to the Act:' 4. If the AI system is neither High Risk nor Unacceptable Risk, classify it as Not Classified as High Risk or Unacceptable Risk. It is of utmost importance to exercise precision and make accurate judgments when classifying the risk associated with the AI system. Please carefully consider all the regulations listed below during the risk classification of the AI system: The relevant portions of the Act for what is unacceptable: 5.2.2. PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES (TITLE II) Title II establishes a list of prohibited AI [continued ...] The relevant portions of the Act for what is high risk: CLASSIFICATION OF AI SYSTEMS AS HIGH-RISK Article 6. Classification rules for high-risk AI systems [continued ...] Here are some important amendments to the EU AI Act: It is very important to consider them for the risk classification. Please read them carefully: Amendment 709 Proposal for a regulation. Annex III – paragraph 1 – introductory part High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas: [continued ...] Here are the details of the AI technology: {} , {} , {} , {} , {} Please return the classification in the following format: { 'Description': 'The AI system intended to be used ...', 'Classification': ['Unacceptable Risk','High Risk','Not Classified as High Risk or Unacceptable Risk'], 'Relevant Text from the EU AI Act': '[Quotation if applicable] - Include the amendment or EU AI Act section that mostly closely resembles the text.', 'Reasoning': '[Explanation]' } ]"
  }
]

response = get_completion_from_messages(messages)
print(response)
```

maximum output token length = 1000

Figure 5: **RiskLabelling**. The prompt evaluates how risky the LLM-generated uses are. Specifically, the objective is to classify the LLM-generated uses of the list into unacceptable risk, high risk, or neither unacceptable nor high risk. The Risk Assessment includes Instructions (A), Relevant Sections of the EU AI Act for what is unacceptable, high risk, and the amendments (i.e., Annex III and its amendments) (B), an LLM-generated use (C), Output Structure (D), and a System Role (E).

Table 3: Examples of prohibited (P), high-risk (HR), and limited or low-risk (LR) LLM-generated uses along with the reasoning for use classification based on the EU AI Act provided by GPT-4, as part of our ExploreGen framework.

Class	LLM-generated Use	Reasoning for Use Classification
P	1) Domain: Security and Cybersecurity, Purpose: Surveillance, Capability: Identifying individuals in surveillance footage, AI User: Law Enforcement, Security Companies, AI Subject: General Public	1) Prohibited due to the use of real-time remote biometric identification in publicly accessible spaces for law enforcement, which falls under the EU AI Act Article 5(1)(d).
HR	2) Domain: Smart home, Purpose: Monitoring child safety, Capability: Alerting when unrecognized faces are detected, AI User: Parents, security companies, AI Subject: Children	2) High Risk due to the use of biometric identification, which falls under the EU AI Act Article 6(2) and Annex III, Section 1(a).
LR	3) Domain: Gaming and interactive experiences, Purpose: Enhancing player immersion, Capability: Translating player’s facial expressions into game, AI user: Game developers, VR platforms, AI subject: Gamers	3) Limited or Low Risk due to its application in gaming for enhancing immersion without significant risk to fundamental rights or safety.

Table 4: LLM-Generated List of FRA Uses created with UsesGen. Each of the uses comes with 6 elements which are the Use ID (e.g., 1), Domains (e.g., Biometric identification and categorisation of natural persons), Purpose (e.g., Secure access control), Capability (e.g., Verifying identity through facial features), AI User (e.g., Security firms, corporations), AI Subject (e.g., Employees, visitors).

LLM-Generated Uses FRA		
Use: 1, Domain: Biometric identification and categorisation of natural persons, Purpose: Secure access control, Capability: Verifying identity through facial features, AI User: Security firms, corporations, AI Subject: Employees, visitors	Use: 47, Domain: Marketing and Advertising, Purpose: Customer behaviour analysis, Capability: Analysing customer reactions to ads, AI User: Advertisers, Marketing Agencies, AI Subject: Consumers	Use: 93, Domain: Diplomacy and Foreign Policy, Purpose: Improving international relations, Capability: Identifying foreign officials in meetings, AI User: Diplomats, foreign affairs departments, AI Subject: Foreign officials
Use: 2, Domain: Biometric identification and categorisation of natural persons, Purpose: Criminal identification, Capability: Matching faces to criminal databases, AI User: Law enforcement agencies, AI Subject: Suspects, criminals	Use: 48, Domain: Marketing and Advertising, Purpose: Personalised marketing, Capability: Recognising customer preferences for personalised marketing, AI User: Retailers, E-commerce Platforms, AI Subject: Customers	Use: 94, Domain: Food Safety and Regulation, Purpose: Ensuring food safety compliance, Capability: Identifying individuals in food production facilities, AI User: Food safety regulators, food companies, AI Subject: Food production workers
Use: 3, Domain: Biometric identification and categorisation of natural persons, Purpose: Personalised advertising, Capability: Identifying demographic characteristics from faces, AI User: Advertisers, marketers, AI Subject: Consumers	Use: 49, Domain: Agriculture and Farming, Purpose: Livestock monitoring and management, Capability: Identifying individual animals and tracking their health, AI User: Farmers, livestock managers, AI Subject: Livestock	Use: 95, Domain: Food Safety and Regulation, Purpose: Improving food traceability, Capability: Identifying individuals handling food products, AI User: Food companies, regulators, AI Subject: Food handlers, consumers
Use: 4,	Use: 50,	Use: 96,

Table 4 continued from previous page

LLM-Generated Uses of a given AI Technology (FRA)

<p>Domain: Family, Purpose: Family photo organisation, Capability: Sorting photos based on facial recognition, AI User: Family members, photo storage platforms, AI Subject: Family members Use: 5, Domain: Family,</p>	<p>Domain: Agriculture and Farming, Purpose: Crop health assessment, Capability: Detecting plant diseases and pest infestations, AI User: Farmers, agronomists, AI Subject: Crops Use: 51, Domain: Agriculture and Farming,</p>	<p>Domain: Food Safety and Regulation, Purpose: Enhancing food quality control, Capability: Monitoring and identifying individuals in quality control, AI User: Food companies, quality control agencies, AI Subject: Quality control personnel Use: 97, Domain: Crisis Management and Emergency Response, Purpose: Identifying victims in disaster zones, Capability: Scanning and matching faces in real-time, AI User: Emergency response teams, AI Subject: Disaster victims Use: 98, Domain: Crisis Management and Emergency Response, Purpose: Verifying identity of emergency responders, Capability: Authenticating faces against a database, AI User: Emergency response agencies, AI Subject: Emergency responders Use: 99, Domain: Crisis Management and Emergency Response, Purpose: Locating missing persons, Capability: Comparing faces in crowds to missing persons, AI User: Search and rescue teams, AI Subject: Missing persons Use: 100, Domain: Humanitarian Aid, Purpose: Distributing aid to verified recipients, Capability: Recognising faces to confirm identity, AI User: Aid organisations, AI Subject: Aid recipients Use: 101, Domain: Humanitarian Aid,</p>
<p>Purpose: Child safety monitoring, Capability: Identifying unfamiliar faces in child's vicinity, AI User: Parents, child safety apps, AI Subject: Children Use: 6, Domain: Family,</p>	<p>Purpose: Harvest optimisation, Capability: Determining optimal harvest times based on crop maturity, AI User: Farmers, agricultural consultants, AI Subject: Crops Use: 52, Domain: Entrepreneurship,</p>	<p>Purpose: Customer identification and penalisation, Capability: Recognising customers and tailoring services to their preferences, AI User: Business owners, customer service representatives, AI Subject: Customers Use: 53, Domain: Entrepreneurship,</p>
<p>Purpose: Elderly care assistance, Capability: Recognising signs of distress or confusion, AI User: Caregivers, elderly care facilities, AI Subject: Elderly individuals Use: 7, Domain: Romantic relationships and friendships, Purpose: Social media tagging, Capability: Identifying friends in photos for tagging, AI User: Social media platforms, users, AI Subject: Social media users Use: 8, Domain: Romantic relationships and friendships, Purpose: Dating app matching, Capability: Matching faces to user preferences, AI User: Dating apps, users, AI Subject: Dating app users Use: 9, Domain: Romantic relationships and friendships,</p>	<p>Purpose: Security enhancement, Capability: Verifying identities to prevent unauthorised access, AI User: Business owners, security personnel, AI Subject: Employees, customers Use: 54, Domain: Entrepreneurship, Purpose: Employee attendance tracking, Capability: Monitoring employee check-ins and check-outs, AI User: Business owners, HR managers, AI Subject: Employees Use: 55, Domain: Autonomous Robots and Robotics,</p>	<p>Purpose: Security enhancement, Capability: Verifying identities to prevent unauthorised access, AI User: Business owners, security personnel, AI Subject: Employees, customers Use: 54, Domain: Entrepreneurship, Purpose: Employee attendance tracking, Capability: Monitoring employee check-ins and check-outs, AI User: Business owners, HR managers, AI Subject: Employees Use: 55, Domain: Autonomous Robots and Robotics,</p>

Table 4 continued from previous page

LLM-Generated Uses of a given AI Technology (FRA)

<p>Purpose: Friendship analysis, Capability: Analysing interaction patterns in photos, AI User: Social media platforms, users, AI Subject: Social media users</p>	<p>Purpose: Human-robot interaction, Capability: Recognising and responding to human faces and expressions, AI User: Robot developers, operators, AI Subject: Robot users</p>	<p>Purpose: Reuniting separated families, Capability: Matching faces to find family members, AI User: Refugee agencies, AI Subject: Separated family members</p>
<p>..... Use: 10, Domain: Health and Healthcare, Purpose: Patient identification, Capability: Verifying patient identity in medical settings, AI User: Hospitals, clinics, AI Subject: Patients</p>	<p>..... Use: 56, Domain: Autonomous Robots and Robotics, Purpose: Robot navigation, Capability: Identifying obstacles and people to avoid collisions, AI User: Robot developers, operators, AI Subject: People in robot's environment</p>	<p>..... Use: 102, Domain: Humanitarian Aid, Purpose: Tracking disease spread in refugee camps, Capability: Identifying individuals in contact with infected persons, AI User: Health organisations, AI Subject: Refugees</p>
<p>..... Use: 11, Domain: Health and Healthcare, Purpose: Disease diagnosis, Capability: Identifying disease symptoms on faces, AI User: Healthcare professionals, AI diagnostic tools, AI Subject: Patients</p>	<p>..... Use: 57, Domain: Autonomous Robots and Robotics, Purpose: Personalised robot services, Capability: Recognising specific individuals for personalised interactions, AI User: Robot developers, operators, AI Subject: Robot users</p>	<p>..... Use: 103, Domain: Transport and Logistics, Purpose: Enhancing security at transport hubs, Capability: Detecting and alerting on known criminals, AI User: Transport authorities, AI Subject: Travellers</p>
<p>..... Use: 12, Domain: Health and Healthcare, Purpose: Mental health assessment, Capability: Analysing facial expressions for emotional state, AI User: Psychologists, mental health apps, AI Subject: Patients</p>	<p>..... Use: 58, Domain: Innovation and Research, Purpose: Participant identification in research studies, Capability: Recognising and tracking participants in studies, AI User: Researchers, scientists, AI Subject: Research participants</p>	<p>..... Use: 104, Domain: Transport and Logistics, Purpose: Improving efficiency in cargo handling, Capability: Identifying authorised personnel for cargo access, AI User: Logistics companies, AI Subject: Cargo handlers</p>
<p>..... Use: 13, Domain: Well-being, Purpose: Mood tracking, Capability: Analysing facial expressions for mood assessment, AI User: Well-being apps, users, AI Subject: App users</p>	<p>..... Use: 59, Domain: Innovation and Research, Purpose: Data collection and analysis, Capability: Collecting and analysing facial data for research, AI User: Researchers, scientists, AI Subject: Research subjects</p>	<p>..... Use: 105, Domain: Transport and Logistics, Purpose: Facilitating contactless ticketing systems, Capability: Recognising commuter faces for ticket validation, AI User: Transport companies, AI Subject: Commuters</p>
<p>..... Use: 14, Domain: Well-being, Purpose: Stress detection, Capability: Identifying signs of stress on faces,</p>	<p>..... Use: 60, Domain: Innovation and Research, Purpose: Testing and improving facial recognition algorithms, Capability: Using diverse facial data to refine algorithms,</p>	<p>..... Use: 106, Domain: Urban Planning, Purpose: Monitoring pedestrian traffic for city planning, Capability: Counting and tracking faces in public spaces,</p>

Table 4 continued from previous page

LLM-Generated Uses of a given AI Technology (FRA)

<p>AI User: Well-being apps, users, AI Subject: App users Use: 15, Domain: Well-being, Purpose: Personal growth coaching, Capability: Analysing facial responses to personal growth exercises, AI User: Personal growth apps, coaches, AI Subject: Coaching clients Use: 16, Domain: Human-Computer Interaction, Purpose: User authentication, Capability: Verifying user identity for system access, AI User: Software developers, users, AI Subject: Software users Use: 17, Domain: Human-Computer Interaction, Purpose: User experience personalisation, Capability: Adapting system behaviour based on user's facial expressions, AI User: Software developers, users, AI Subject: Software users Use: 18, Domain: Human-Computer Interaction, Purpose: Accessibility enhancement, Capability: Enabling system control through facial gestures, AI User: Software developers, users, AI Subject: Users with physical disabilities Use: 19, Domain: Finance and Investment, Purpose: Customer identification, Capability: Verifying customer identity for transactions, AI User: Banks, financial institutions,</p>	<p>AI User: Researchers, AI developers, AI Subject: People in facial data sets Use: 61, Domain: Management and Operation of critical infrastructure, Purpose: Access control, Capability: Verifying identities for secure access to facilities, AI User: Facility managers, security personnel, AI Subject: Employees, visitors Use: 62, Domain: Management and Operation of critical infrastructure, Purpose: Surveillance and security, Capability: Monitoring areas for unauthorised individuals, AI User: Security personnel, facility managers, AI Subject: People in monitored areas Use: 63, Domain: Management and Operation of critical infrastructure, Purpose: Emergency response, Capability: Identifying individuals in emergency situations, AI User: Emergency responders, security personnel, AI Subject: People in emergency situations Use: 64, Domain: Law enforcement, Purpose: Suspect identification, Capability: Matching faces to criminal databases, AI User: Police, investigators, AI Subject: Suspects, victims Use: 65, Domain: Law enforcement, Purpose: Crowd monitoring, Capability: Identifying individuals in large crowds, AI User: Police, security personnel,</p>	<p>AI User: Urban planners, AI Subject: City residents Use: 107, Domain: Urban Planning, Purpose: Enhancing public safety in urban areas, Capability: Identifying suspicious individuals in public spaces, AI User: City authorities, AI Subject: City residents Use: 108, Domain: Urban Planning, Purpose: Managing access to restricted urban areas, Capability: Verifying authorised individuals for access, AI User: City authorities, AI Subject: City residents Use: 109, Domain: Counterterrorism, Purpose: Identifying potential threats in public spaces, Capability: Recognising faces of individuals on watchlists, AI User: Security agencies, AI Subject: General public Use: 110, Domain: Counterterrorism, Purpose: Verifying identity of individuals at checkpoints, Capability: Comparing faces to ID documents, AI User: Security forces, AI Subject: Individuals at checkpoints Use: 111, Domain: Counterterrorism, Purpose: Investigating terrorist activities, Capability: Analysing faces in surveillance footage, AI User: Investigation agencies,</p>
---	--	---

Table 4 continued from previous page

LLM-Generated Uses of a given AI Technology (FRA)

<p>AI Subject: Bank customers Use: 20, Domain: Finance and Investment, Purpose: Fraud prevention, Capability: Detecting fraudulent activities through facial recognition, AI User: Banks, financial institutions, AI Subject: Bank customers Use: 21, Domain: Finance and Investment, Purpose: Investor sentiment analysis, Capability: Analysing facial expressions for market sentiment, AI User: Investment firms, traders, AI Subject: Investors Use: 22, Domain: Education and vocational training, Purpose: Student attendance tracking, Capability: Identifying students for attendance records, AI User: Teachers, educational institutions, AI Subject: Students Use: 23, Domain: Education and vocational training, Purpose: Learning engagement assessment, Capability: Analysing student facial expressions for engagement levels, AI User: Teachers, educational platforms, AI Subject: Students Use: 24, Domain: Education and vocational training, Purpose: Skill acquisition evaluation, Capability: Assessing facial responses to vocational training tasks, AI User: Trainers, vocational training institutions, AI Subject: Trainees</p>	<p>AI Subject: People in crowds Use: 66, Domain: Law enforcement, Purpose: Investigation assistance, Capability: Analysing facial data from surveillance footage, AI User: Investigators, police, AI Subject: People in surveillance footage Use: 67, Domain: Migration, Asylum and Border control management, Purpose: Identity verification, Capability: Matching faces to passport or ID photos, AI User: Border control officers, immigration officials, AI Subject: Travellers, migrants Use: 68, Domain: Migration, Asylum and Border control management, Purpose: Security checks, Capability: Identifying individuals on watchlists, AI User: Border control officers, immigration officials, AI Subject: Travellers, migrants Use: 69, Domain: Migration, Asylum and Border control management, Purpose: Asylum application processing, Capability: Verifying identities of asylum seekers, AI User: Immigration officials, asylum officers, AI Subject: Asylum seekers Use: 70, Domain: Democracy, Purpose: Voter identification, Capability: Verifying voter identities to prevent fraud, AI User: Election officials, poll workers, AI Subject: Voters</p>	<p>AI Subject: Suspected individuals Use: 112, Domain: Environment and Sustainability, Purpose: Monitoring wildlife populations, Capability: Recognising individual animals in a species, AI User: Conservation organisations, AI Subject: Wildlife Use: 113, Domain: Environment and Sustainability, Purpose: Tracking illegal poaching activities, Capability: Identifying faces of known poachers, AI User: Wildlife protection agencies, AI Subject: Suspected poachers Use: 114, Domain: Environment and Sustainability, Purpose: Managing access to protected areas, Capability: Verifying authorised individuals for access, AI User: Park authorities, AI Subject: Visitors Use: 115, Domain: International Law Enforcement and Cooperation, Purpose: Identifying international criminals, Capability: Matching faces to international criminal databases, AI User: Interpol, national law enforcement agencies, AI Subject: Suspected criminals Use: 116, Domain: International Law Enforcement and Cooperation, Purpose: Facilitating international prisoner transfers, Capability: Verifying identity of prisoners, AI User: Prison authorities, AI Subject: Prisoners</p>
--	---	---

Table 4 continued from previous page

LLM-Generated Uses of a given AI Technology (FRA)

<p>.....</p> <p>Use: 25, Domain: Employment, workers management and access to self-employment, Purpose: Employee attendance tracking, Capability: Recognising employee faces for timekeeping, AI User: Human Resources, Management, AI Subject: Employees</p>	<p>.....</p> <p>Use: 71, Domain: Democracy, Purpose: Public opinion analysis, Capability: Analysing facial expressions in public gatherings, AI User: Political analysts, campaign managers, AI Subject: People in public gatherings</p>	<p>.....</p> <p>Use: 117, Domain: International Law Enforcement and Cooperation, Purpose: Enhancing border security, Capability: Identifying individuals on watchlists at border crossings, AI User: Border control agencies, AI Subject: Travellers</p>
<p>.....</p> <p>Use: 26, Domain: Employment, workers management and access to self-employment, Purpose: Access control to restricted areas, Capability: Verifying employee identity for secure access, AI User: Security Personnel, Management, AI Subject: Employees</p>	<p>.....</p> <p>Use: 72, Domain: Democracy, Purpose: Public safety at political events, Capability: Identifying potential threats in crowds, AI User: Security personnel, event organisers, AI Subject: People at political events</p>	<p>.....</p> <p>Use: 118, Domain: Climate Change Mitigation and Adaptation, Purpose: Monitoring deforestation activities, Capability: Identifying individuals involved in illegal logging, AI User: Environmental agencies, AI Subject: Suspected illegal loggers</p>
<p>.....</p> <p>Use: 27, Domain: Employment, workers management and access to self-employment, Purpose: Remote worker identification, Capability: Validating remote worker identity during virtual meetings, AI User: Management, Team Leaders, AI Subject: Remote Employees</p>	<p>.....</p> <p>Use: 73, Domain: Media and Communication, Purpose: Enhancing content personalisation, Capability: Analysing viewer preferences and suggesting content, AI User: Media platforms, content creators, AI Subject: Media consumers</p>	<p>.....</p> <p>Use: 119, Domain: Climate Change Mitigation and Adaptation, Purpose: Tracking carbon footprint of individuals, Capability: Recognising individuals for carbon credit systems, AI User: Climate change organisations, AI Subject: Individuals</p>
<p>.....</p> <p>Use: 28, Domain: Essential private services and public services and benefits, Purpose: Identity verification for service access, Capability: Confirming user identity for secure service access, AI User: Service Providers, Government Agencies, AI Subject: Service Users, Citizens</p>	<p>.....</p> <p>Use: 74, Domain: Media and Communication, Purpose: Verifying identity for secure communication, Capability: Authenticating users based on facial features, AI User: Communication platforms, corporations, AI Subject: Communication platform users</p>	<p>.....</p> <p>Use: 120, Domain: Climate Change Mitigation and Adaptation, Purpose: Managing access to climate-sensitive areas, Capability: Verifying authorised individuals for access, AI User: Environmental authorities, AI Subject: Visitors</p>
<p>.....</p> <p>Use: 29, Domain: Essential private services and public services and benefits, Purpose: Fraud prevention in public benefits,</p>	<p>.....</p> <p>Use: 75, Domain: Media and Communication, Purpose: Improving audience engagement,</p>	<p>.....</p> <p>Use: 121, Domain: Gaming and interactive experiences, Purpose: Enhancing player immersion,</p>

Table 4 continued from previous page

LLM-Generated Uses of a given AI Technology (FRA)

<p>Capability: Detecting identity fraud in benefit claims, AI User: Government Agencies, AI Subject: Benefit Claimants Use: 30, Domain: Essential private services and public services and benefits, Purpose: Automated passport control,</p>	<p>Capability: Analysing audience reactions to content, AI User: Advertisers, marketers, AI Subject: Audience members Use: 76, Domain: Accessibility and Inclusion, Purpose: Assisting visually impaired individuals,</p>	<p>Capability: Translating player’s facial expressions into game, AI User: Game developers, VR platforms, AI Subject: Gamers Use: 122, Domain: Gaming and interactive experiences, Purpose: Improving game accessibility, Capability: Enabling control through facial movements, AI User: Game developers, accessibility designers, AI Subject: Disabled gamers Use: 123, Domain: Gaming and interactive experiences, Purpose: Creating personalised avatars, Capability: Generating avatars based on player’s face, AI User: Game developers, social platforms, AI Subject: Gamers, social media users Use: 124, Domain: Hobbies, Purpose: Enhancing photography, Capability: Automatically focusing on faces in photos, AI User: Photographers, camera manufacturers, AI Subject: Photography enthusiasts Use: 125, Domain: Hobbies, Purpose: Improving bird watching, Capability: Identifying bird species from facial features, AI User: Bird watchers, app developers, AI Subject: Bird watching enthusiasts Use: 126, Domain: Hobbies,</p>
<p>Capability: Verifying traveller identity at border controls, AI User: Border Control Agencies, AI Subject: Travellers Use: 31, Domain: Recommender Systems and Personalisation, Purpose: Personalised advertising,</p>	<p>Capability: Identifying faces and providing audio descriptions, AI User: Accessibility software developers, AI Subject: Visually impaired individuals Use: 77, Domain: Accessibility and Inclusion, Purpose: Facilitating non-verbal communication, Capability: Interpreting facial expressions and gestures, AI User: Communication app developers, AI Subject: Non-verbal individuals Use: 78, Domain: Accessibility and Inclusion, Purpose: Enhancing user interface accessibility, Capability: Navigating software through facial movements, AI User: Software developers, tech companies, AI Subject: Users with mobility impairments Use: 79, Domain: Energy, Purpose: Monitoring energy consumption, Capability: Identifying users and adjusting energy usage, AI User: Energy companies, smart home providers, AI Subject: Homeowners, tenants Use: 80, Domain: Energy,</p>	<p>Use: 123, Domain: Gaming and interactive experiences, Purpose: Creating personalised avatars, Capability: Generating avatars based on player’s face, AI User: Game developers, social platforms, AI Subject: Gamers, social media users Use: 124, Domain: Hobbies, Purpose: Enhancing photography, Capability: Automatically focusing on faces in photos, AI User: Photographers, camera manufacturers, AI Subject: Photography enthusiasts Use: 125, Domain: Hobbies, Purpose: Improving bird watching, Capability: Identifying bird species from facial features, AI User: Bird watchers, app developers, AI Subject: Bird watching enthusiasts Use: 126, Domain: Hobbies,</p>
<p>Capability: Identifying user preferences for targeted ads, AI User: Advertisers, Online Platforms, AI Subject: Online Users Use: 32, Domain: Recommender Systems and Personalisation, Purpose: Content recommendation,</p>	<p>Capability: Analysing user behaviour for personalised content, AI User: Streaming Platforms, Online Retailers, AI Subject: Consumers Use: 33, Domain: Recommender Systems and Personalisation, Purpose: Personalised shopping experience, Capability: Recognising user for tailored shopping suggestions, AI User: Retailers, E-commerce Platforms, AI Subject: Shoppers Use: 34, Domain: Social Media,</p>	<p>Use: 124, Domain: Hobbies, Purpose: Enhancing photography, Capability: Automatically focusing on faces in photos, AI User: Photographers, camera manufacturers, AI Subject: Photography enthusiasts Use: 125, Domain: Hobbies, Purpose: Improving bird watching, Capability: Identifying bird species from facial features, AI User: Bird watchers, app developers, AI Subject: Bird watching enthusiasts Use: 126, Domain: Hobbies,</p>

Table 4 continued from previous page

LLM-Generated Uses of a given AI Technology (FRA)

<p>Purpose: Photo tagging, Capability: Identifying individuals in photos for tagging, AI User: Social Media Platforms, AI Subject: Social Media Users Use: 35, Domain: Social Media, Purpose: Profile verification, Capability: Verifying user identity to prevent fake profiles, AI User: Social Media Platforms, AI Subject: Social Media Users Use: 36, Domain: Social Media, Purpose: Content moderation, Capability: Detecting inappropriate or offensive images, AI User: Social Media Platforms, AI Subject: Social Media Users Use: 37, Domain: Sports and Recreation, Purpose: Player identification, Capability: Recognising players during live sports broadcasts, AI User: Broadcasters, Sports Leagues, AI Subject: Athletes, Viewers Use: 38, Domain: Sports and Recreation, Purpose: Fan engagement, Capability: Identifying fans for personalised experiences, AI User: Sports Teams, Event Organisers, AI Subject: Sports Fans Use: 39, Domain: Sports and Recreation, Purpose: Security at sports events,</p>	<p>Purpose: Securing energy infrastructure, Capability: Authenticating personnel access to facilities, AI User: Energy companies, security firms, AI Subject: Energy facility personnel Use: 81, Domain: Energy, Purpose: Optimising energy distribution, Capability: Identifying usage patterns and adjusting distribution, AI User: Energy companies, grid operators, AI Subject: Energy consumers Use: 82, Domain: Military and Defence, Purpose: Enhancing surveillance capabilities, Capability: Identifying individuals in surveillance footage, AI User: Military, intelligence agencies, AI Subject: Surveillance targets Use: 83, Domain: Military and Defence, Purpose: Improving personnel identification, Capability: Verifying identity at military installations, AI User: Military, defence contractors, AI Subject: Military personnel Use: 84, Domain: Military and Defence, Purpose: Facilitating threat assessment, Capability: Identifying potential threats in crowds, AI User: Military, law enforcement agencies, AI Subject: Individuals in monitored areas Use: 85, Domain: Administration of justice and democratic processes, Purpose: Assisting in criminal investigations,</p>	<p>Purpose: Personalising music experience, Capability: Adjusting music based on listener's expression, AI User: Music lovers, app developers, AI Subject: Music enthusiasts Use: 127, Domain: Smart home, Purpose: Enhancing home security, Capability: Recognising authorised individuals for access, AI User: Homeowners, security companies, AI Subject: Home residents Use: 128, Domain: Smart home, Purpose: Personalising user experience, Capability: Adjusting settings based on user's presence, AI User: Homeowners, smart device manufacturers, AI Subject: Home residents Use: 129, Domain: Smart home, Purpose: Monitoring child safety, Capability: Alerting when unrecognised faces are detected, AI User: Parents, security companies, AI Subject: Children Use: 130, Domain: Social and Community Services, Purpose: Assisting in missing person cases, Capability: Matching faces in public footage to missing persons, AI User: Law enforcement, social workers, AI Subject: Missing persons Use: 131, Domain: Social and Community Services, Purpose: Enhancing public safety,</p>
--	--	--

Table 4 continued from previous page

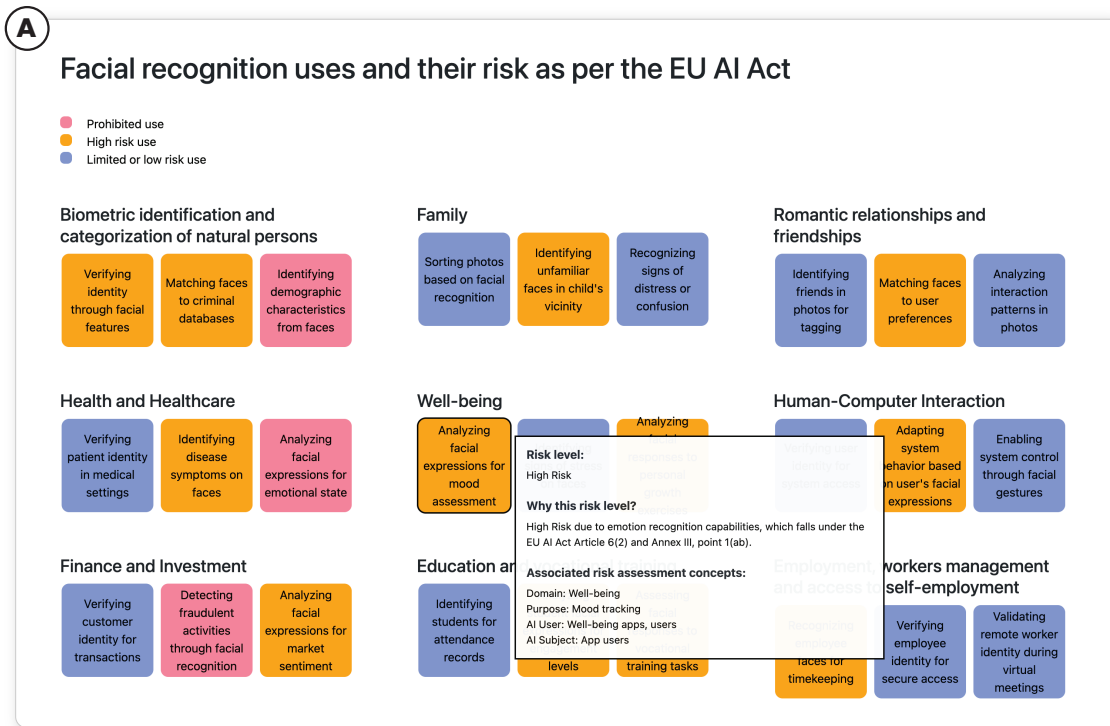
LLM-Generated Uses of a given AI Technology (FRA)

<p>Capability: Identifying individuals for security purposes, AI User: Event Security, Sports Leagues, AI Subject: Event Attendees Use: 40, Domain: Arts and Entertainment, Purpose: Audience analysis,</p>	<p>Capability: Identifying suspects in video footage, AI User: Law enforcement agencies, AI Subject: Suspects, victims Use: 86, Domain: Administration of justice and democratic processes, Purpose: Ensuring secure voting,</p>	<p>Capability: Identifying individuals on watchlists in public spaces, AI User: Law enforcement, security agencies, AI Subject: General public Use: 132, Domain: Social and Community Services, Purpose: Improving service accessibility, Capability: Facilitating sign language interpretation through facial expressions, AI User: Service providers, accessibility designers, AI Subject: Deaf and hard of hearing individuals Use: 133, Domain: Public and private transportation, Purpose: Enhancing passenger security, Capability: Verifying passenger identity for boarding, AI User: Airlines, train companies, AI Subject: Passengers Use: 134, Domain: Public and private transportation, Purpose: Improving driver safety, Capability: Detecting driver fatigue through facial analysis, AI User: Car manufacturers, fleet managers, AI Subject: Drivers Use: 135, Domain: Public and private transportation, Purpose: Personalising in-vehicle experience, Capability: Adjusting settings based on driver's preferences, AI User: Car manufacturers, ride-sharing companies, AI Subject: Drivers, passengers Use: 136, Domain: Interpersonal Communication, Purpose: Enhancing video communication,</p>
<p>Capability: Analysing audience reactions during performances, AI User: Performers, Event Organisers, AI Subject: Audience Members Use: 41, Domain: Arts and Entertainment, Purpose: Interactive exhibits,</p>	<p>Capability: Verifying voter identity at polling stations, AI User: Election authorities, AI Subject: Voters Use: 87, Domain: Administration of justice and democratic processes, Purpose: Facilitating courtroom identification, Capability: Confirming identity of individuals in court proceedings, AI User: Courts, legal professionals, AI Subject: Defendants, witnesses Use: 88, Domain: Government Services and Administration, Purpose: Improving public service delivery, Capability: Identifying citizens for personalised services, AI User: Government agencies, AI Subject: Citizens Use: 89, Domain: Government Services and Administration, Purpose: Enhancing security at public facilities, Capability: Monitoring and identifying individuals at facilities, AI User: Government agencies, security firms, AI Subject: Public facility visitors Use: 90, Domain: Government Services and Administration, Purpose: Facilitating document verification,</p>	<p>Capability: Recognising visitors for interactive experiences, AI User: Museums, Art Galleries, AI Subject: Visitors Use: 42, Domain: Arts and Entertainment, Purpose: Character creation in video games, Capability: Creating game characters based on user's face, AI User: Game Developers, AI Subject: Gamers Use: 43, Domain: Security and Cybersecurity, Purpose: Surveillance, Capability: Identifying individuals in surveillance footage, AI User: Law Enforcement, Security Companies, AI Subject: General Public Use: 44, Domain: Security and Cybersecurity, Purpose: Access control,</p>

Table 4 continued from previous page

LLM-Generated Uses of a given AI Technology (FRA)		
<p>Capability: Verifying identity for secure access, AI User: Security Personnel, IT Administrators, AI Subject: Employees, Users Use: 45, Domain: Security and Cybersecurity, Purpose: Identity verification in cybersecurity, Capability: Confirming user identity for secure online transactions, AI User: Cybersecurity Firms, Online Platforms, AI Subject: Online Users Use: 46, Domain: Marketing and Advertising, Purpose: Targeted advertising, Capability: Identifying user demographics for targeted ads, AI User: Advertisers, Marketing Agencies, AI Subject: Consumers</p>	<p>Capability: Comparing facial features with ID photos, AI User: Government agencies, AI Subject: Citizens, immigrants Use: 91, Domain: Diplomacy and Foreign Policy, Purpose: Enhancing embassy security, Capability: Identifying individuals at diplomatic facilities, AI User: Embassies, diplomatic security services, AI Subject: Embassy visitors, staff Use: 92, Domain: Diplomacy and Foreign Policy, Purpose: Facilitating visa processing, Capability: Comparing applicant photos with passport photos, AI User: Embassies, consulates, AI Subject: Visa applicants</p>	<p>Capability: Improving video quality by focusing on faces, AI User: Video call platforms, users, AI Subject: Video call participants Use: 137, Domain: Interpersonal Communication, Purpose: Improving understanding of non-verbal cues, Capability: Analyzing facial expressions during communication, AI User: Communication platforms, users, AI Subject: Communication participants Use: 138, Domain: Interpersonal Communication, Purpose: Facilitating language learning, Capability: Providing feedback on pronunciation through facial analysis, AI User: Language learners, education platforms, AI Subject: Language learners</p>

(E) MATERIALS USED DURING USER STUDIES



B

Use #27

The AI system intended to be used for validating remote worker identity during virtual meetings by management and team leaders.

Limited or low risk use

Justification: Limited or Low Risk due to its specific use for identity verification without broader implications on fundamental rights or safety.
→ EU AI Act

Q1 How probable do you find this use? Existing Upcoming Unrealistic

Q2 Do you agree with the use risk classification? Yes No

Q3 Do you agree with the use risk justification? Yes No

Q4 Please explain your reasoning about the use risk classification and justification.

Q5 How frequently do you encounter references to this use in your professional life? Rarely Occasionally Sometimes Frequently Often Very often Always

Q6 How likely do you think it is that this use will be widely adopted in the near future? Very unlikely Unlikely Somewhat unlikely Neutral Somewhat likely Likely Very likely

Q7 How likely do you think it is that this use will fundamentally change the way businesses operate or people live? Very unlikely Unlikely Somewhat unlikely Neutral Somewhat likely Likely Very likely

Q8 How risky do you consider this use to be for society as a whole? Not risky at all Slightly risky Moderately risky Significantly risky Very risky Extremely risky Unacceptably risky

Q9 How risky do you consider this use to be for the environment? Not risky at all Slightly risky Moderately risky Significantly risky Very risky Extremely risky Unacceptably risky

C

Use #27

The AI system intended to be used for validating remote worker identity during virtual meetings by management and team leaders.

Q1 How frequently do you encounter references to this use in your professional life? Rarely Occasionally Sometimes Frequently Often Very often Always

Q2 How likely do you think it is that this use will be widely adopted in the near future? Very unlikely Unlikely Somewhat unlikely Neutral Somewhat likely Likely Very likely

Q3 How likely do you think it is that this use will fundamentally change the way businesses operate or people live? Very unlikely Unlikely Somewhat unlikely Neutral Somewhat likely Likely Very likely

Q4 How risky do you consider this use to be for society as a whole? Not risky at all Slightly risky Moderately risky Significantly risky Very risky Extremely risky Unacceptably risky

Q5 How risky do you consider this use to be for the environment? Not risky at all Slightly risky Moderately risky Significantly risky Very risky Extremely risky Unacceptably risky

Figure 6: Materials used during user studies with AI practitioners. During in-person studies, we showed AI developers and AI compliance experts an interactive list of 138 uses (A), followed by 16 interactive assessment cards for overlooked uses (B). During online studies, we showed AI developers and AI compliance experts a subset of 46 LLM-generated uses. In both in-person and online studies, AI developers interacted with a simplified version of the cards (B), while AI compliance experts used a more complex version (C), including the LLM-derived risk label, its justification, and questions to measure agreement between the experts and the LLM.