Note

To : European Commission & AI HLEG
From: Professors Susan Perry and Claudia Roda
Date: June 11, 2020
Re: Comments on EC White Paper on AI

The European Commission's February 2020 *'White Paper on Artificial Intelligence: a European approach to excellence and trust'* is focused on 'trustworthy' artificial intelligence, with the laudable perspective that European citizens and businesses will be more likely to invest in and use 'trustworthy' AI. Rather than echo industrial discourse on the trustworthiness of technology, the White Paper's market-driven approach to AI must be reinforced by robust, practical protection of the fundamental rights and freedoms guaranteed in the 2012 EU Charter of Fundamental Rights. This Note will make four recommendations to render human rights protection **actionable** with respect to AI for citizens and business in the European Union.

The lifecycle of an AI product is complex, and includes both the software and hardware necessary for its functionality. The SHERPA Stakeholder Board has been tasked with reflecting on technical and regulatory options for the ethical use of AI throughout a product lifecycle. Our reflection begins with a product's inception; the analysis of the algorithms necessary for its functionality; the framework for its lifecycle; data access, use and storage; the integration of one software component with other AI systems; and also includes the ethical implications of the mining, manufacture and recycling of all hardware; plus the integration of renewable energy sources and the evaluation of possible impact on citizens' health. The SHERPA Stakeholder Board has already produced seminal work on these issues, work that is designed to create an ecosystem of excellence for the ethical use of AI.

In the case of complex technology, sometimes the best solution for enhanced human rights protection may be near-at-hand and cost effective. The following four-step process takes advantage of existing patent and data protection infrastructure, while introducing AI support and a powerful new EU agency, in order to render an ecosystem of excellence for the ethical use of AI a reality.

1. **Enhanced patent procedures**. During work for PRIPARE, an FP7 project on privacy-by-design, we targeted the **inception phase** as key to assuring respect for human rights in the design of IT software. We should do the same in order to create trustworthy artificial intelligence.

   Nearly all AI algorithms and software systems are **patented**, sometimes by a novice software designer, sometimes by a large multinational corporation. Each of the European Union Member States has its own national patent office. Moreover, since 1978 a European patent procedure has grouped certain patent applications (all EU member states have joined

the European Patent Convention), whereas WIPO oversees adherence to international intellectual property rights protection. Consequently, the registration of any AI patent presents an opportunity for obligatory adherence to international and European human rights standards.

An automated human rights procedure should accompany any algorithm, software or AI-applicable patent registration. The individual or business filing the patent must guarantee that their product does not in any foreseeable way violate fundamental rights and freedoms. This would function like any due diligence procedure in the pharmaceutical industry, for example, with an understanding that not all potential uses of a product may be anticipated. Nonetheless, the individual or business that files to register an AI product with the intention of making a profit would be required to review the human rights impact of their product and guarantee, to the best of their knowledge, that their product will respect the international and European human rights framework, in particular the following six fundamental rights elaborated in the 2012 Charter and necessary for trustworthy IA use:

- Protection from all forms of discrimination (Title III, Equality)
- Right to life (Title II, Articles 2, 3)
- Right to be free from torture (Title 2, Articles 4, 5)
- Right to privacy (Title II, Articles 6,7, 8)
- Freedom of thought and expression (Title II, Articles 10, 11, 13)
- Freedom of association (Title II, Article 12)

2. **Due diligence oversight**. Each of the EU Member States already has in place oversight bodies for Internet security and data protection. A complaint or redress mechanism through a national watchdog institution (e.g., a Computer Emergency Response Team, a national data protection authority, or a national Human Rights Institution) would enable citizens, civil society or the government to bring a case before a small arbitration panel of 3 experts, who would be tasked with determining whether the AI patent in question adhered to the human rights guarantees made when filing. The panel's jurisdiction would be fairly narrow, but panel experts would be empowered to investigate a complaint and to temporarily suspend a patent if they could establish a pattern of gross or systematic violation with respect to one (or more) of the six fundamental rights mentioned above.

In the case of the France, for example, the **CNIL** (*Commission Nationale de l'Informatique et des Libertés*) has a broad mandate to guarantee citizens' rights with regard to information technology; the CNIL could house France's redress mechanism through a rotating panel of human rights and AI experts. France's national judicial systems would be responsible for any criminal activity or civil damages alleged to have occurred.

Open source software for AI poses a first challenge to this procedure in that there is no patent registration process. Nonetheless, the open source platform could require anyone

uploading software to fill out an online form guaranteeing that the human rights impact of their software has been thought-through, particularly with respect to the six fundamental rights and freedoms.

Military use of AI is outside the scope of the EC White Paper. Nonetheless, dual use technology poses a second challenge with respect to ethical AI use. Most dual use technology (with both a civilian and military application, such as a weather station satellite) must adhere to patent procedures, consequently the individual or business filing the patent registration would still be required to guarantee human rights protections with respect to civilian use.

3. **Specialised software** to support both the enhanced patent procedures and the due diligence oversight. The software would use machine learning to provide tools capable of answering normative questions about compliance with existing laws, regulations and the international human right framework. Patent applicants would thus receive assistance to better understand and respond to appropriate human rights requirements for their AI software and software systems, while national watchdog institutions would be supported in their investigation and assessment of complaints.

   The software could also serve as repository for AI patents and patent requests along with an archive of complaints and arbitration.

4. Finally, a **European Agency for Artificial Intelligence** should be created to monitor both patent registration procedures for AI, as well as the due diligence arbitration procedures by the national data protection bodies. While a regulator might, at first glance, appear to be the most feasible strategy moving forward, the scale and scope of artificial intelligence promises to dwarf most other industries in Europe in the decades to come. If Europe hopes to compete with the United States and China in the AI realm, then more than one individual will be necessary to assure that European AI is excellent, trustworthy and meets the highest international and European human rights standards. The increase in cost will be more than compensated by the reach of a full agency, particularly at the outset of this technology revolution.

***