From: **Adrian Gropper** agropper@healthurl.com
Subject: [Ai-control-workshop-pc] A Delegated Authorization standard for AI access control
Date: July 28, 2024 at 11:34 AM
To: ai-control-workshop-pc@iab.org

Machine Learning and Artificial Intelligence (AI) is a vastly different use-case than Search and a robots.txt approach would be inadequate. Key differences are:

- Search has a natural network effect whereas AI can be scoped to a context, particularly when private data or trade secrets are involved.
- Search has an implicit purpose: to create a public directory. The purpose of AI can be almost anything.
- Search is typically applied to public data. Because a model can be designed to preserve privacy, AI can more readily request access to protected resources.
- Search access control is simple and efficient as befits 30 year-old technology. AI access control can benefit from today's more capable networks and servers.
- Although Search as a service can be manipulated by operators to create "filter bubbles", AI services are much more personal and more susceptible to bias and discrimination.

Prior consent mechanisms such as static robots.txt files do not allow sufficient control to the resource owner, regardless of whether the resource being served is public or private. A modern alternative based on delegated authorization such as IETF GNAP https://datatracker.ietf.org/doc/draft-ietf-gnap-core-protocol/ enables the resource owner to control access dynamically, based on who's asking and for what purpose. An Authorization Server standard can enable both corporate and personal AI at scale and facilitate human-AI alignment through both market-driven and regulatory impact.

Our HIE of One project has over a decade of experience and participation in standards for delegated authorization and regulations over control of private data such as HIPAA and "Patient Right of Access" mandates. Our standards work included contributions to Kantara UMA, W3C Decentralized Identifiers and Verifiable Credentials, as well as GNAP. Health-related use-cases are particularly well-suited to understanding the role of delegated authorization in terms of human-AI alignment. The principal relationship in healthcare is between an individual physician as a fiduciary of an individual patient. Institutional and vendor roles are, by design, secondary to the humans because the responsibility of hospitals, payers, and technology vendors is to their boards and stockholders. Although human fiduciary relationships are a minority of the transactions people engage in, standards that promote delegated authorization to both human and corporate clients could be the foundation of human-AI alignment.

Experience with health information technology and regulation teaches the value of using the same standard for access control across both institutional and personal AI clients. When a standard is designed to serve both institutional and personal tech, strategic manipulation of "privacy" policies and regulatory capture by corporate interests becomes more evident and harder to justify.

As CTO of Patient Privacy Rights Foundation, member of the Electronic Privacy Information Center Advisory Board, and Invited Expert to some W3C workgroups, I hope to participate in this important workshop.

[redacted]