Legal Infrastructure for AI Agent Transactions

Daniel "Dazza" Greenwood
Civics.Com Consultancy, Founder
MIT Media Lab, law.MIT.edu, Executive Director
Stanford Law School, CodeX, Research Affiliate

Version: 2025-03-14

Dazza Greenwood

Civics.Com & law.MIT.edu

"I am passionate about enhancing productivity and creativity with generative AI. At law.MIT.edu, I lead research and publishing endeavors to explore AI's applications in the legal sector. Through my consultancy, Civics.Com, I have trained thousands of lawyers and other professionals on the use of generative AI and directly assist companies in adopting AI to refine their processes and innovate their products, services, and business models."

Legal Dimensions of Agentic AI

Agentic AI

My Background

1999

http://www.civics.com/content/agents/eta_rpt.htm Go JUL JUN 13 AUG
32 captures 2001 2002 2003
11 Jan 2000 – 8 Aug 2007 About this capture

MEMORANDUM

To: Uniform Electronic Transactions Act Drafting Committee;
Professor Patricia B. Fry, Chair and Professor Benjamin Beard, Reporter

From: ABA Section of Business Law, Cyberspace Law Committee Electronic Commerce Subcommittee Working Group on Electronic Contracting Practices Co-Chairs: Daniel Greenwood (dan@civics.com) and John Muller (jmuller@brobeck.com) (fn1)

Date: February 16, 1999

Subject: Preliminary Draft Report on UETA Legal Treatment of Electronic Agents

1. Introduction

This document is a revised draft (fn2) of the meeting proceedings of the Electronic Contracting Practices Working Group at the American Bar Association's Cyberspace Law Committee meeting in Atlanta January 15-16, 1999. The Working Group is focusing its efforts on a survey of legal issues arising from the deployment of electronic agents for business purposes, including considerations of commercial, agency, intellectual property and tort law. As part of this survey, the Working Groups is monitoring and commenting upon developments in UCC Articles 2, 2B and the UETA with respect to Electronic Agents. An initial rough draft of this document was presented on January 16th to Benjamin Beard, UETA Reporter, who has subsequently requested a more formal submission for consideration by the UETA drafting committee in time for the upcoming February 19-21, 1999 drafting Committee meeting in Richmond, VA.

This document first explores the definition currently used in the UETA for Electronic Agent, and then examines the core operative legal rule in the current and immediately prior draft of the UETA, along with a tentative proposed rule developed by the Working Group at the Atlanta meeting. Next, the extent to which operations of an electronic agent should be attributed to a user are discussed, followed by a query about the advisability of developing different operative rules for tool-like vs. intelligent electronic agents (or, possibly, simply limiting application of the UETA to non-intelligent systems). Clearly, other sections of the UETA as well as other NCCUSL draft products also deal with use of electronic agents, however, at this time the Working Group has limited comments to the provisions noted due to the preliminary nature of this draft.

2. UETA Definitions

January 29, 1999 UETA definition of electronic agent (Section 102(8)):

"Electronic agent" means a computer program, electronic, or other automated means used to initiate or respond to electronic records or performances in whole or in part without review by an individual.

Working Group commentary: The emphasis in the definition on review by an individual may call for clarification that review occurring at any point after completion of the record or performance does not cause a program to fall outside this definition.

2011

*YOU ARE CURRENTLY BROWSING THE **CORPBOTS** CATEGORY*

CORPBOTS SEEK ROBO-FRIENDLY FUNDING

§ June 1st, 2011 § Filed under Corpbots § No Comments

Greetings everyone! For all of those who came out to our New and Emerging Legal Infrastructures Conference in April, thank you. We had an extraordinary turnout of lawyers, technologists, and other good folks — and we're still buzzing over here at headquarters about some of the tremendously exciting cross-disciplinary discussions that emerged during the panels.

In the intervening month of May, the partners over here at Robot, Robot & Hwang have been sifting through a variety of different project ideas and trying to figure out what we'll be doing as we move into the summer months out here in the Bay Area. In partnership with our collaborator Dazza Greenwood (his corresponding cross-post here) the senior partners have settled on a direction and glad to say we can go public with what we've been scheming about.

Glad to announce today that we're officially looking for funding to pursue the deployment of the **Corpbot Project**, a flexible, open-source toolkit for developers to easily program *autonomous corporations*.

What is an autonomous corporation you might ask? We've been thinking for some time it'd be amazing

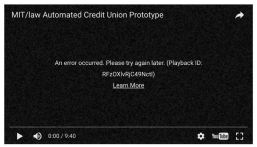
2016

law.MIT.edu
Computational Law Research and Development at MIT

Automated Credit Union for Digital Assets

June 8, 2016

2016-06-28 UPDATE: Today, MIT/law published a short video project overview of the Automated Credit Union Prototype open source project. The video is embedded below:



MIT/law launched the Automated Credit Union Prototype Project today (June 8, 2016) in Washington, DC at the Georgetown University Law Center.

The approach for this exploratory research and development project will be an open source, participatory and collaborative. The key concept is to build a prototype that can test whether an automated US Federally Chartered Credit Union would be well suited to provide member services for personal data and individual identity. Key postulates are that the existing US Credit Union legal/regulatory rules, market/business roles and social/cultural context would require no material changes to exist as automated entities or to provide data and identity services.

2019

View on GitHub

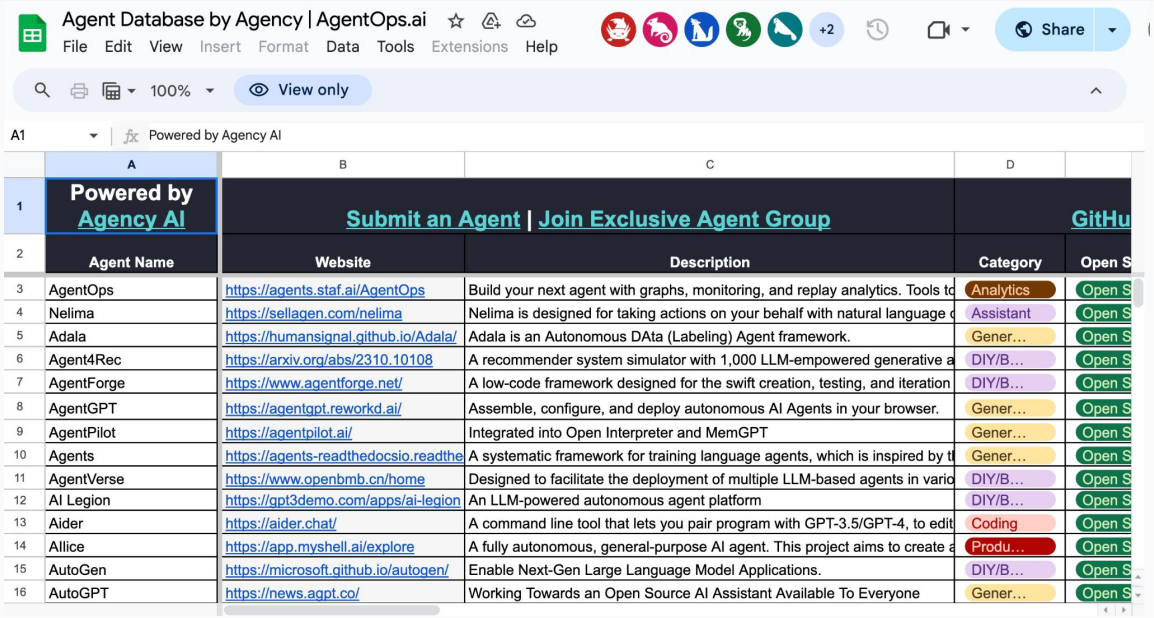
AALE

Automated and Autonomous Legal Entities

AALE: Automated and Autonomous Legal Entities

This site is an MIT Legal Engineering open, collaborative research project to gather a list of automated and autonomous legal entity examples (eg corporations, LLCs, non-profits, etc). We are seeking to compile a list of any such products and projects, including web-based, blockchain-based, and enterprise implementations. This research may be part of an upcoming publication of the MIT Computational Law Report and may form part of an upcoming summit of people leading such projects planned for April, 2020 at Stanford.

Agentic AI is Here and On the Rise



Agent Database by Agency | AgentOps.ai

File Edit View Insert Format Data Tools Extensions Help

Share

100% View only

A1 Powered by Agency AI

	A	B	C	D	
1	Powered by Agency AI	Submit an Agent | Join Exclusive Agent Group			GitHu
2	Agent Name	Website	Description	Category	Open S
3	AgentOps	https://agents.staf.ai/AgentOps	Build your next agent with graphs, monitoring, and replay analytics. Tools to	Analytics	Open S
4	Nelima	https://sellagen.com/nelima	Nelima is designed for taking actions on your behalf with natural language c	Assistant	Open S
5	Adala	https://humansignal.github.io/Adala/	Adala is an Autonomous DAta (Labeling) Agent framework.	Gener…	Open S
6	Agent4Rec	https://arxiv.org/abs/2310.10108	A recommender system simulator with 1,000 LLM-empowered generative a	DIY/B…	Open S
7	AgentForge	https://www.agentforge.net/	A low-code framework designed for the swift creation, testing, and iteration	DIY/B…	Open S
8	AgentGPT	https://agentgpt.reworkd.ai/	Assemble, configure, and deploy autonomous AI Agents in your browser.	Gener…	Open S
9	AgentPilot	https://agentpilot.ai/	Integrated into Open Interpreter and MemGPT	Gener…	Open S
10	Agents	https://agents-readthedocsio.readthe	A systematic framework for training language agents, which is inspired by th	Gener…	Open S
11	AgentVerse	https://www.openbmb.cn/home	Designed to facilitate the deployment of multiple LLM-based agents in vario	DIY/B…	Open S
12	AI Legion	https://gpt3demo.com/apps/ai-legion	An LLM-powered autonomous agent platform	DIY/B…	Open S
13	Aider	https://aider.chat/	A command line tool that lets you pair program with GPT-3.5/GPT-4, to edit	Coding	Open S
14	Allice	https://app.myshell.ai/explore	A fully autonomous, general-purpose AI agent. This project aims to create a	Produ…	Open S
15	AutoGen	https://microsoft.github.io/autogen/	Enable Next-Gen Large Language Model Applications.	DIY/B…	Open S
16	AutoGPT	https://news.agpt.co/	Working Towards an Open Source AI Assistant Available To Everyone	Gener…	Open S

Example list of 450+ Agentic AI Companies and Products

Legislative Hearings

Agentic AI for Algorithmic Decisions and Transactional Law

- Hearing 1: July 2, 2024
- Hearing 2: September 16, 2024

Testimony on Agentic AI Systems and Automated Decision Making

Testimony to the Wyoming Select Committee (joint House/Senate) Covering "Digital Innovation Technology"

DAZZA GREENWOOD
JUL 02, 2024

5 Share

Yesterday I testified again to a Select Committee of the Wyoming legislature, led by Co-Chairs Senator Rothfuss and Representative Western, on the topic of automated decision making technology in the context of generative AI. We delved into the use of large language models as "agents" who can operate and even conduct transactions on behalf of individuals and organizations. I'm delighted to say this topic will continue to be explored through one of the Select Committees informal drafting groups, resulting in a deeper discussion and perhaps draft legislation at their next hearing this coming autumn.

The testimony can be found here, and is embedded below.

CodeX Research: Contracts & Terms Review

→ Stanford CodeX/HAI/DEL Agent Legal Frameworks

→ Agent Protocols / OpenWeb Paradigm

→ Modular/Interoperable Agents - Gen Spring

→ Autonomous Orgs and New EcoArchitecture

What Could Possibly Go Wrong?

Perhaps this technology is so useful, the main risk is over reliance upon it.

The Harbingers of Liability are Upon Us

POP CULTURE

Prankster tricks a GM chatbot into agreeing to sell him a $76,000 Chevy Tahoe for $1

Maybe the AI revolution has an upside?

By Tod Perry, Upworthy Staff 03.16.24

Reuters World Business Markets More Register

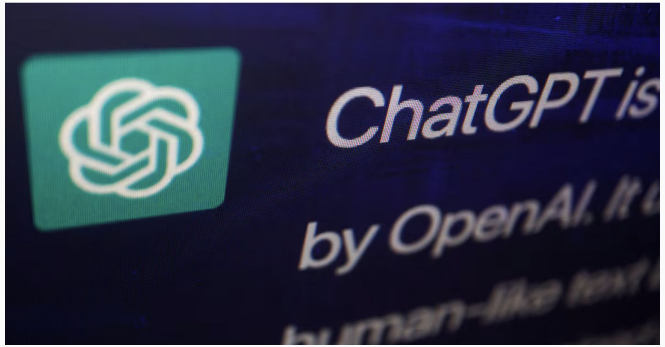
My View Following Saved

Disrupted

New York lawyers sanctioned for using fake ChatGPT cases in legal brief

By Sara Merken

June 26, 2023 3:28 AM CDT · Updated a year ago



WIRED SECURITY POLITICS GEAR MORE SUBSCRIBE

Air Canada Has to Honor a Refund Policy Its Chatbot Made Up

The airline tried to argue that it shouldn't be liable for anything its chatbot says.

Let's Get More Specific About Risks
NIST.AI 600-1 (April, 2024)

- **CBRN Information** (chem, bio, nuclear)
- **Confabulation**
- **Dangerous or Violent Recommendations**
- **Data Privacy**
- **Environmental**
- **Human-AI Configuration:** (transparency, explainability)
- **Information Integrity** (deep fakes)
- **Information Security**
- **Intellectual Property**
- **Obscene, Degrading, and/or Abusive Content**
- **Toxicity, Bias, and Homogenization**
- **Value Chain and Component Integration**

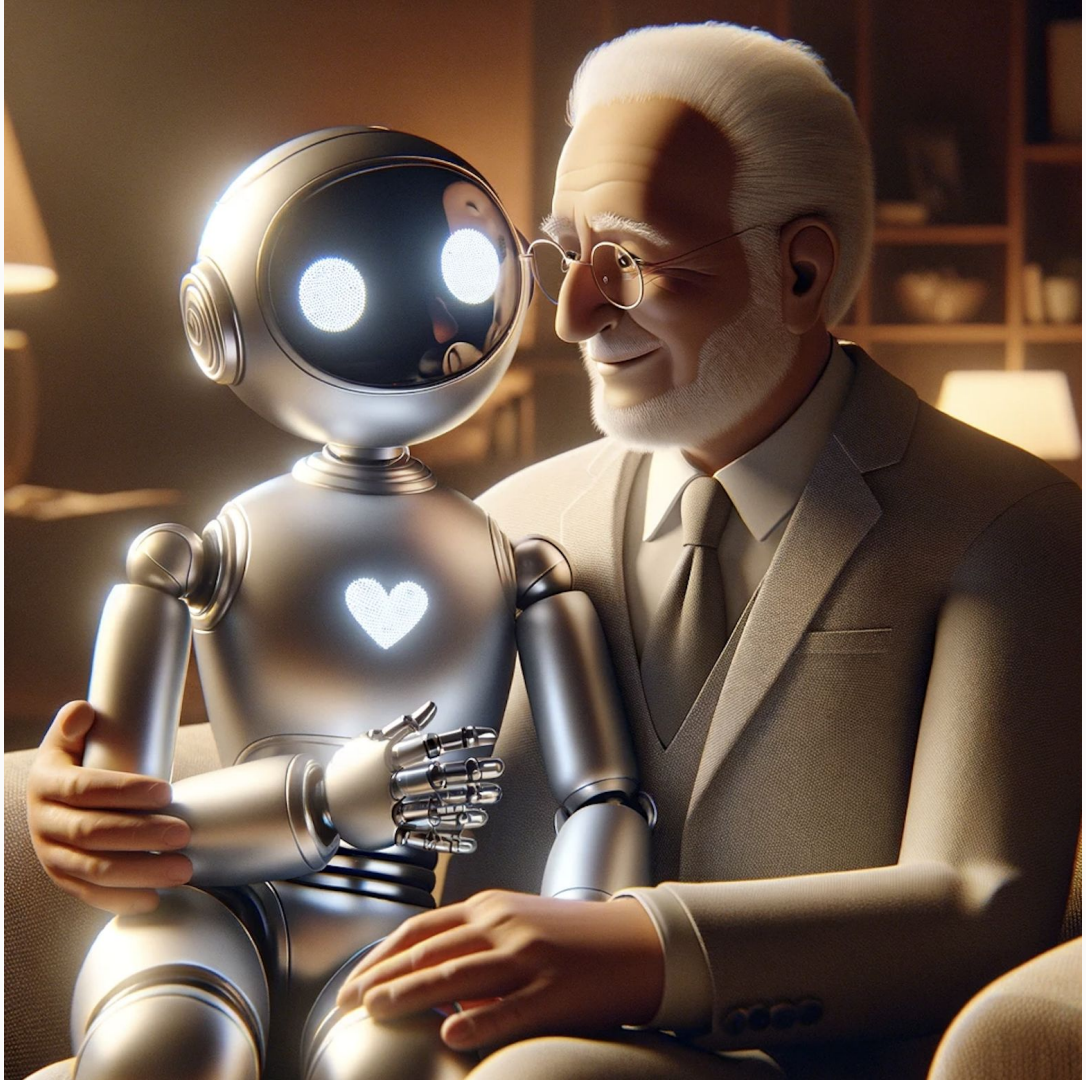
Peter Drucker *on risk*

The risk one must accept, the risk that is built into the nature of the business.

The risk one can afford to take.

The risk one cannot afford to take.

The risk one cannot afford not to take.

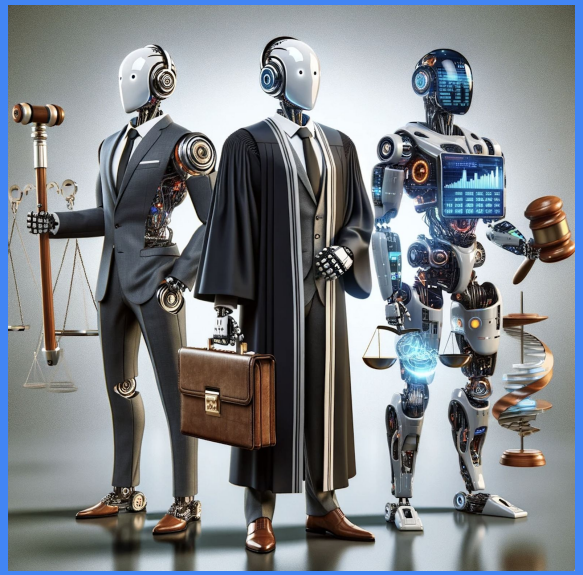


Compliance Implication for Lawyers Using GenAI

The State Bar of California

ABA®

Electronic Agents and Agentic AI



Old-World: High frequency trading relies on electronic agents. These are electronic agents conducting automated transactions, to be sure. Same with a lot of supply chains. Same with payment networks and many other systems.

What's different now?

With generative AI, agentic systems can do something like "think" for themselves. Therefore, they can start to address "in-the-wild" interaction environments. This new capability is perfectly matched to address many of the most intractable challenges to prior electronic agent systems and opens up a lot of single-party, ecommerce, business-to-business, and other contexts.

What are Agentic AI Systems?

- ***Can adaptably achieve complex goals in complex environments with limited direct supervision***
- Are characterized by high degrees of:
  - **Goal complexity:** Ability to achieve challenging and wide-ranging goals
  - **Environmental complexity:** Ability to achieve goals under a wide range of complex environments
  - **Adaptability:** Ability to adapt and react to novel or unexpected circumstances
  - **Independent execution:** Ability to reliably achieve goals with limited (*or no*) human intervention

Demystifying the Nuts and Bolts

Design Patterns

- Chain of Agents
- Master / worker
- Hierarchical teams
- Collaborative teams
- Facilitator / mediator

Mechanics

- Plan → Execute
- Hand-Off
- Routing
- Tool Use
- Shared context / memory

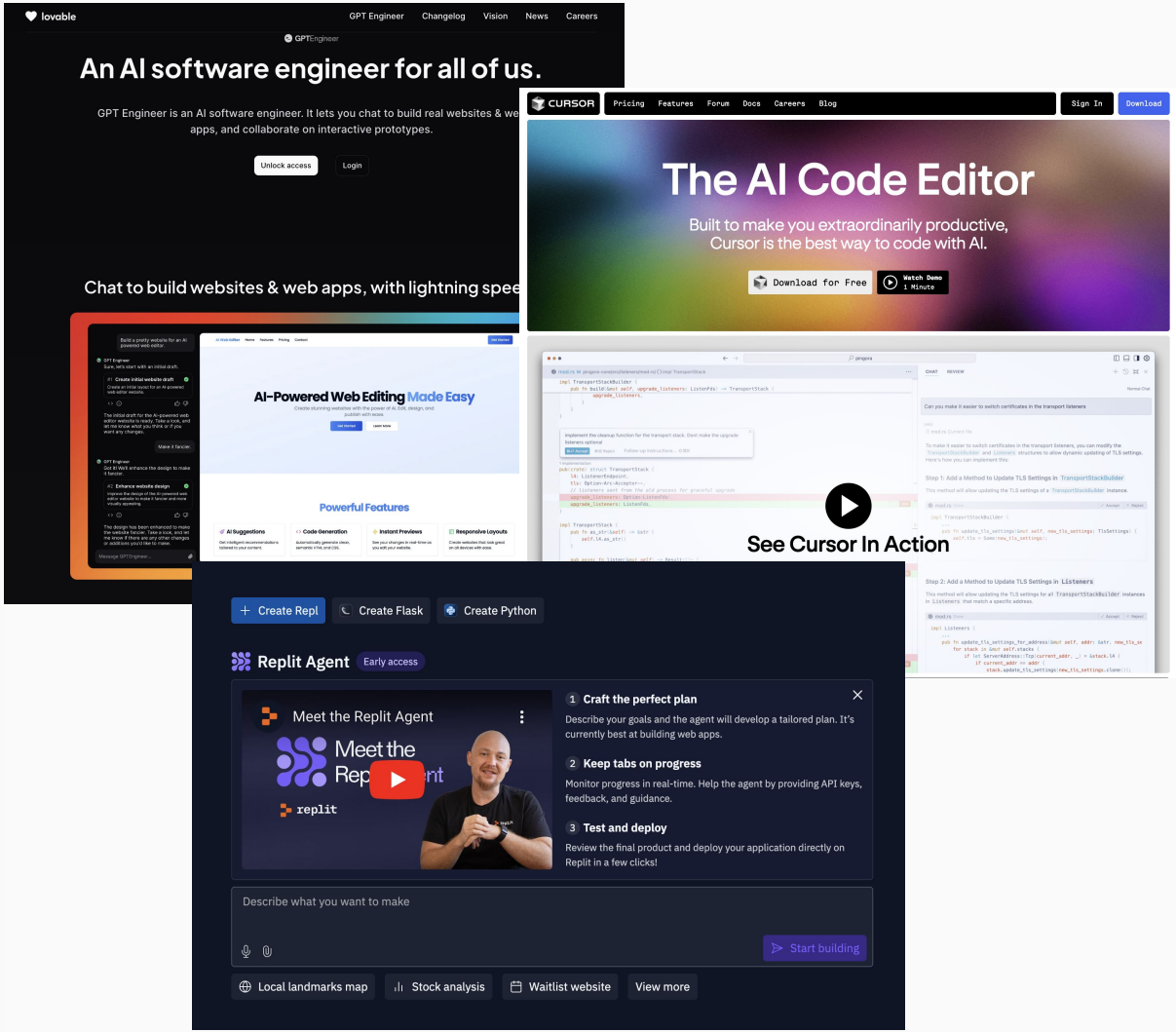
Task & Project Applications

Example
Agentic AI Systems:

Software Developer

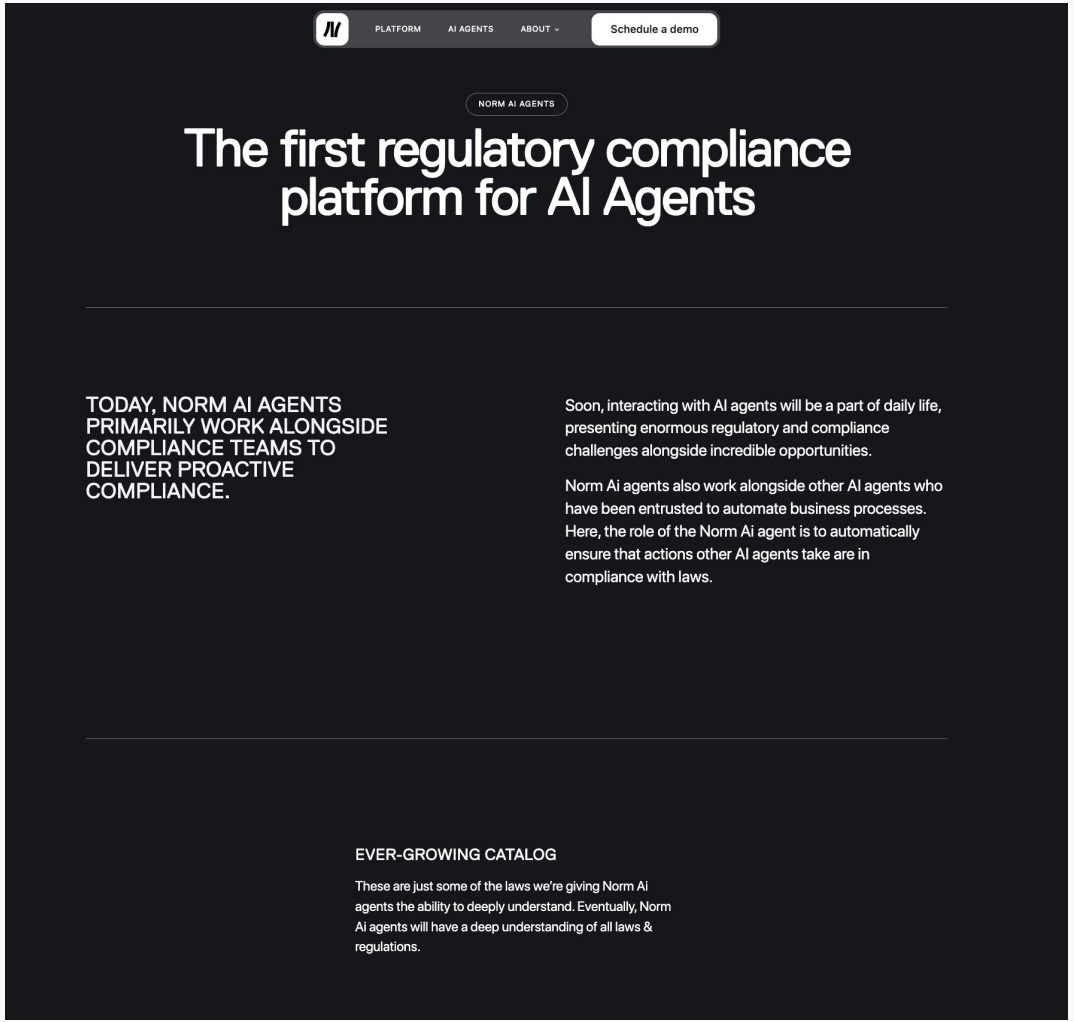
Example
Agentic AI Systems:

Software Developers



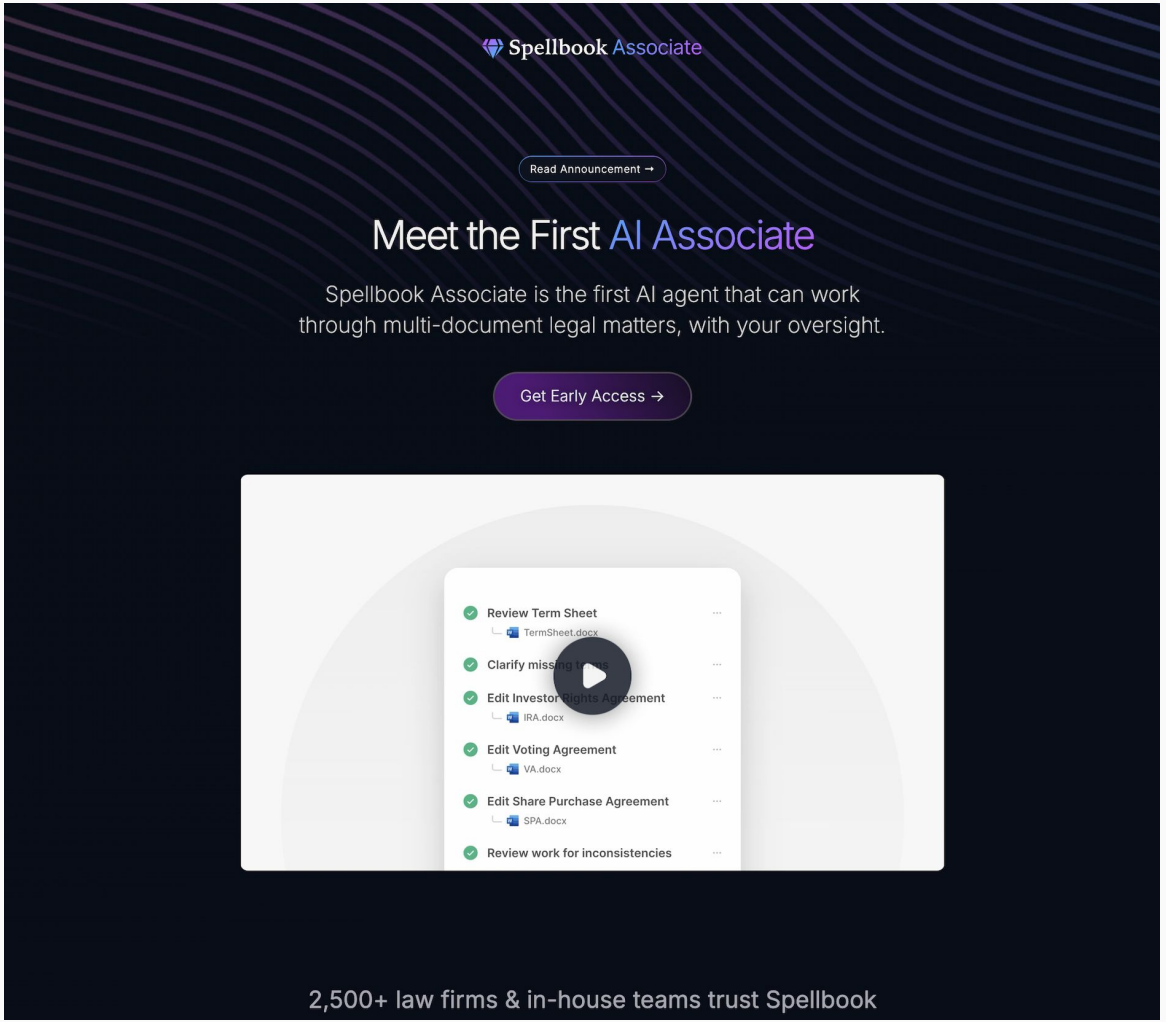
Example
Agentic AI Systems:

Compliance Officer



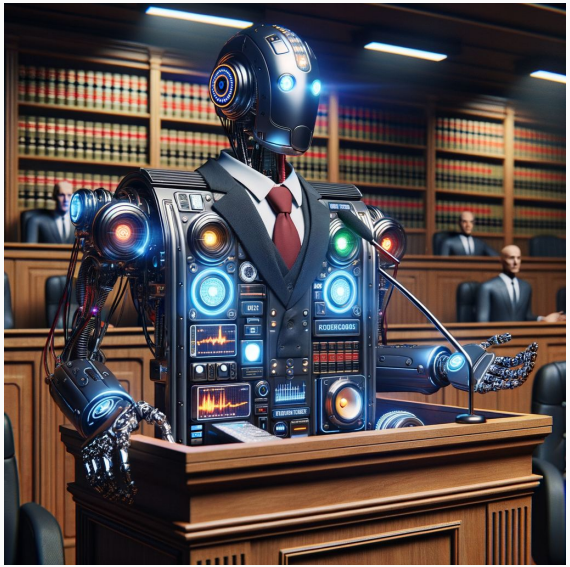
Example
Agentic AI Systems:

Legal Associate

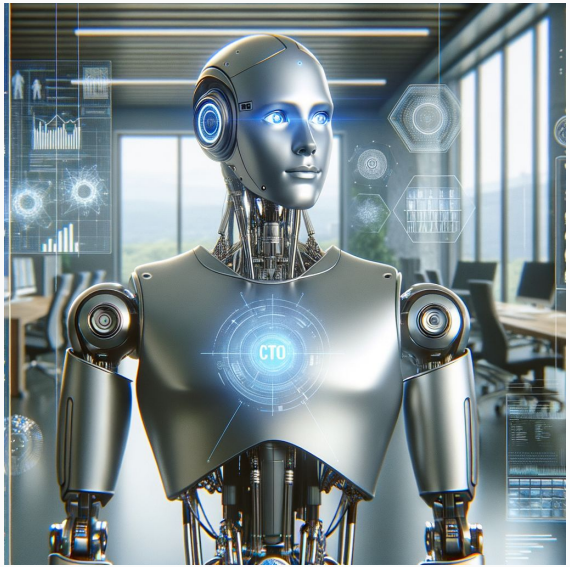


Hybrid Team of Gen AI Agents

Legal Agent

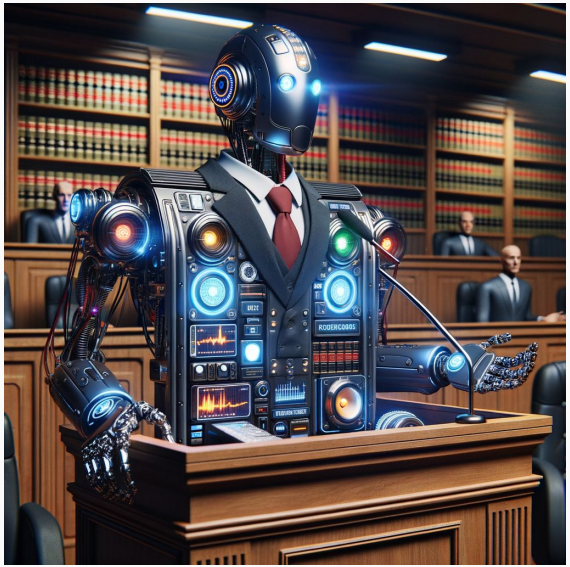


Technical Agent



Hybrid Team of Gen AI Agents

Legal Agent

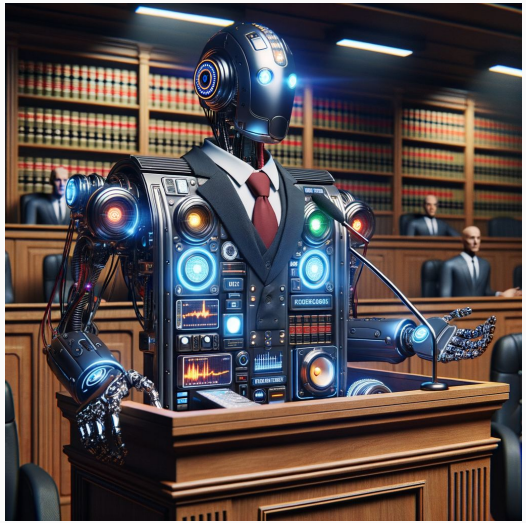


Business Agent

Hybrid Team of Gen AI Agents

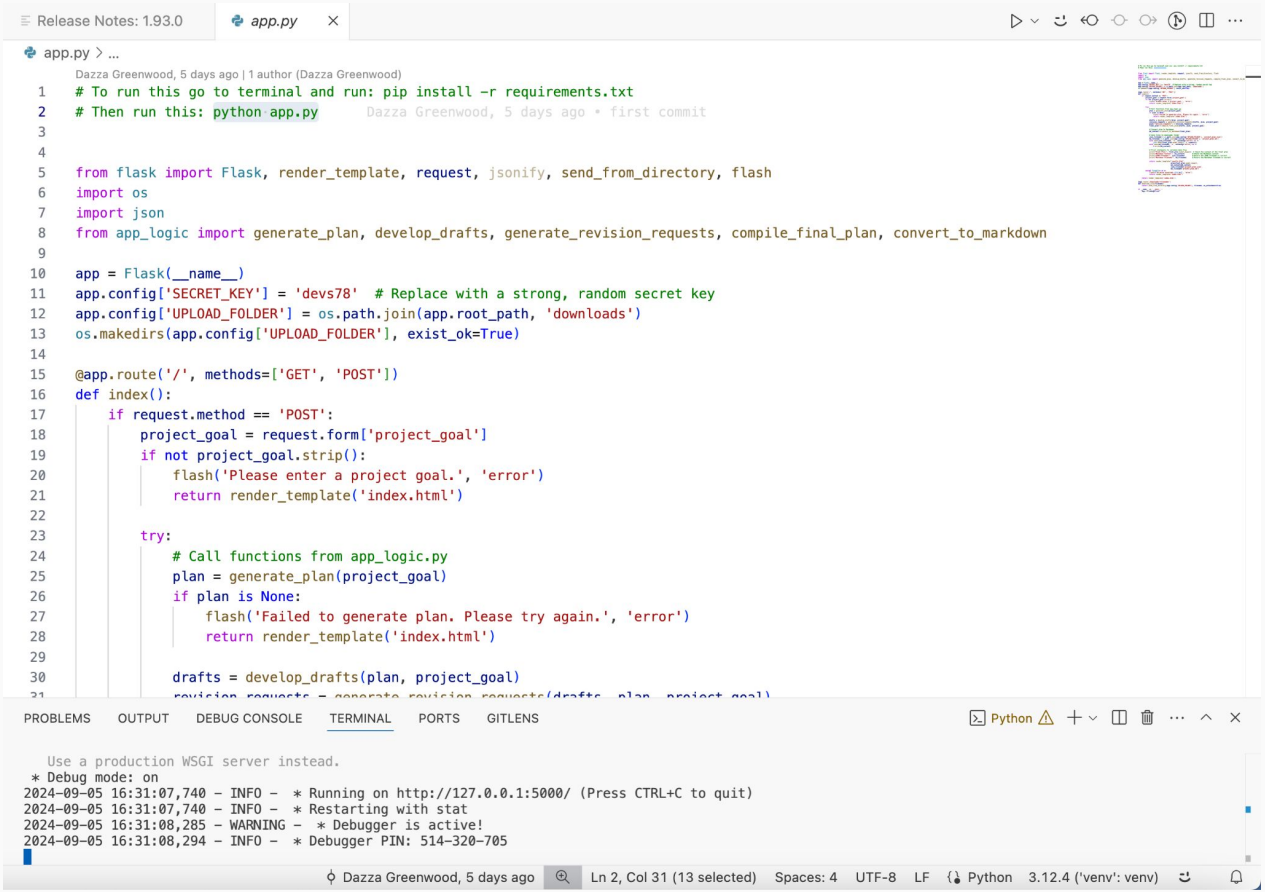
Business Agent

Legal Agent



Technical Agent

Goal to Deliverables: The Agento Prototype of Self-Assembling BLT Project Teams



AI Scientist

sakana.ai

sakana.ai

The AI Scientist: Towards Fully Automated Open-Ended Scientific Discovery

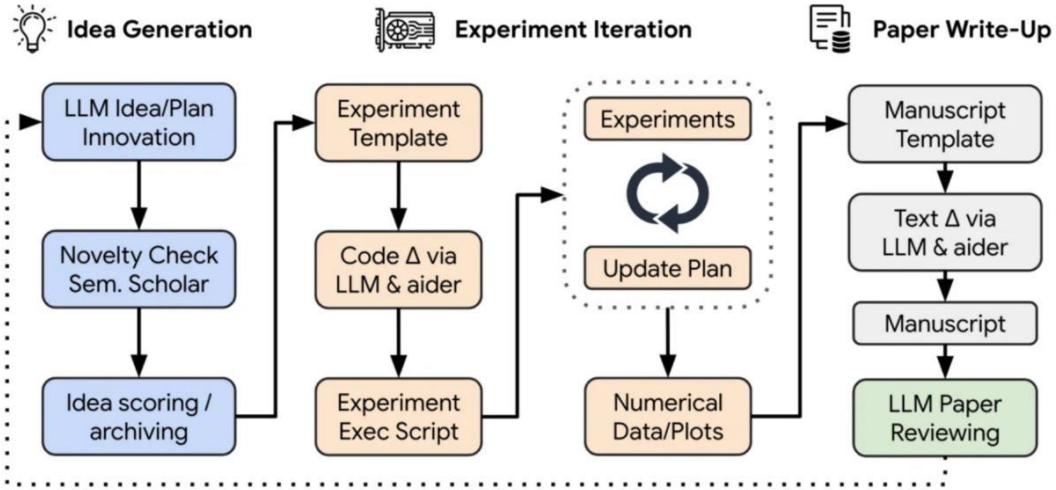
August 13, 2024

Initial PoC of End-to-End Paper Writing

README | Apache-2.0 license

The AI Scientist: Towards Fully Automated Open-Ended Scientific Discovery

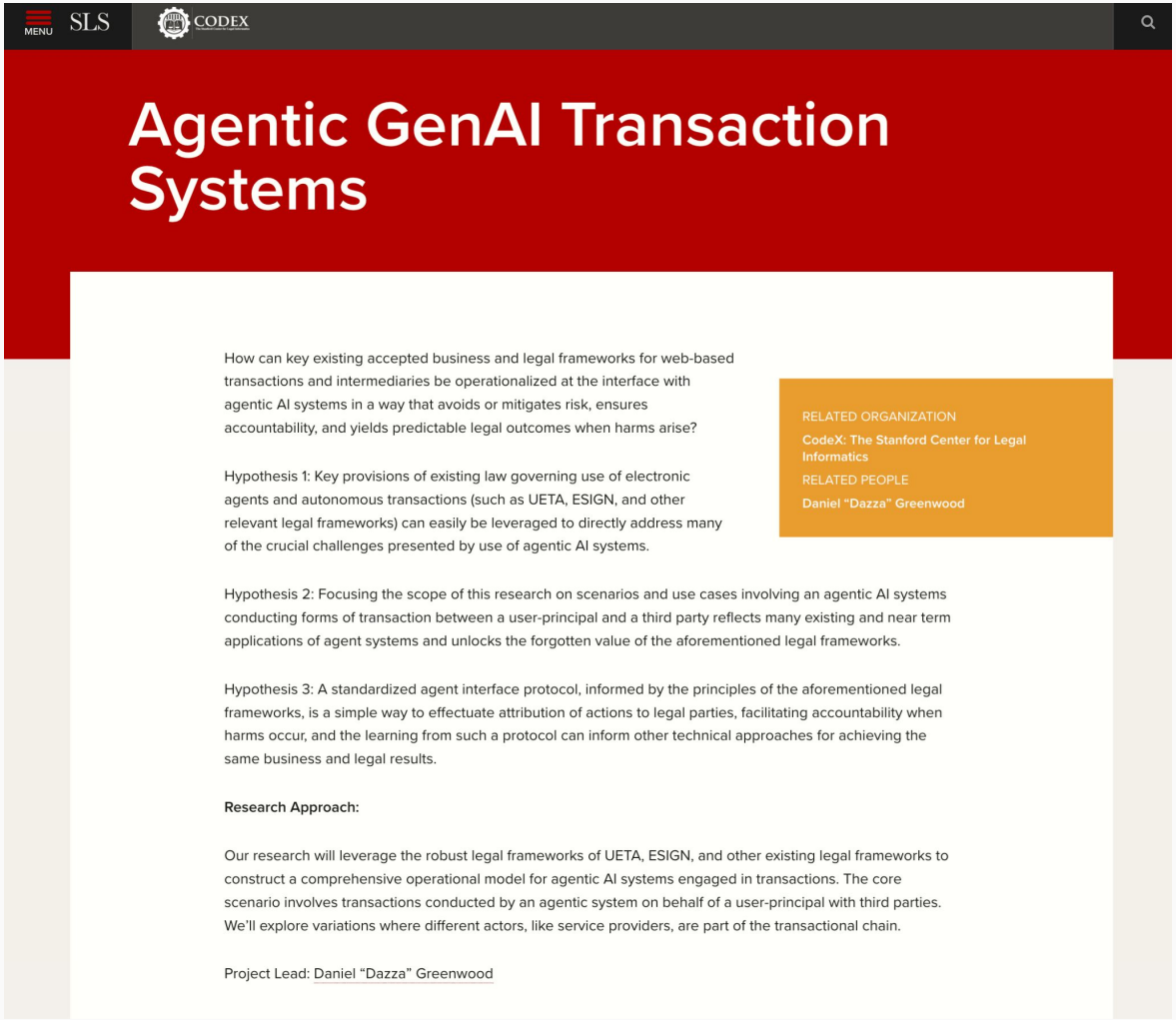
[Paper] | [Blog Post] | [Drive Folder]



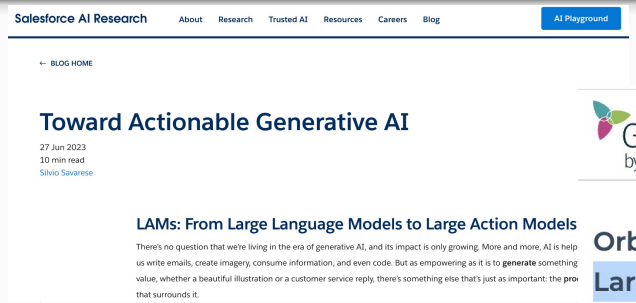
Transactional Applications

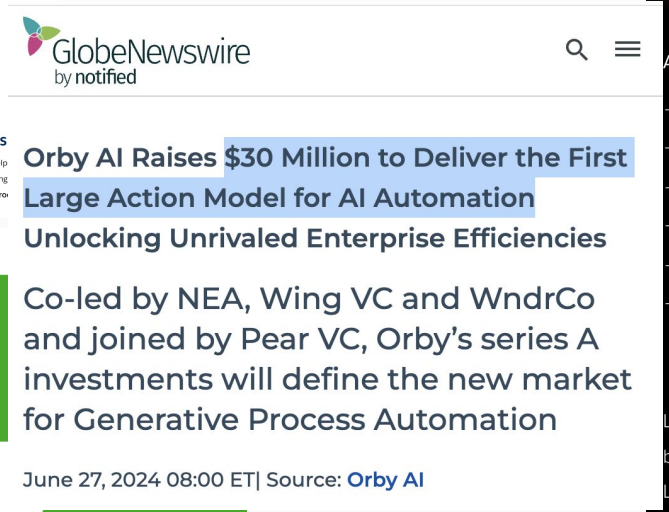
Transactions

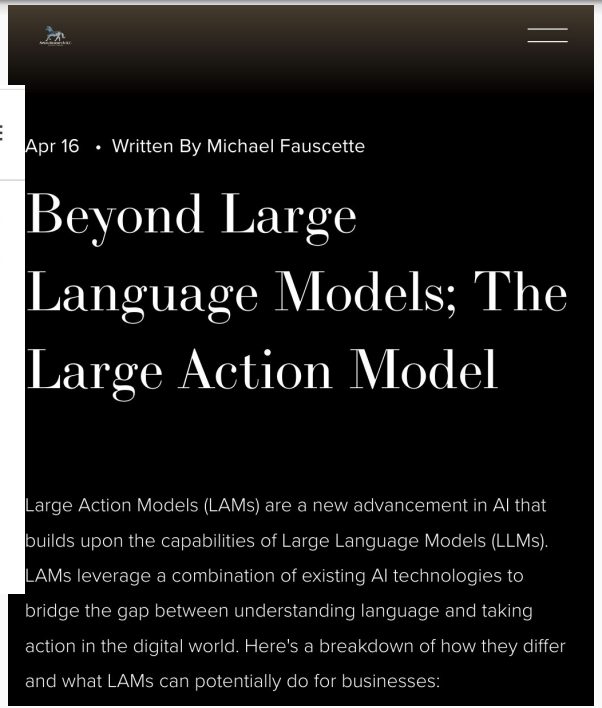
What happens when parts of the actions agentic AI systems perform includes conducting transactions?



The Brief Foray of "Large Action Models"







Basic Existing Transactional Use Cases

Online Shopping Agent: Handles product search, price comparisons, purchases, and delivery arrangements. Legal considerations include e-commerce terms & conditions, return policies, and consumer protection regulations.

Travel Booking Agent: Books flights, accommodations, and transportation based on user preferences and constraints. Legal aspects involve cancellation policies, travel insurance terms, and potential liability issues.

Appointment Scheduling Agent: Manages bookings with service providers like doctors or hairdressers. Legal considerations include adherence to booking site terms and relevant guidelines (e.g., HIPAA for healthcare).

Automated Bill Payment Agent: Ensures timely payments and manages account balances. Key legal aspects include financial regulations and secure handling of sensitive data.

"Actions" to "Interactions" to "Transactions"

Add Agenda Action

Find the Current Price of a Product

Schedule Appointment

SQL Query Action

Tabular Data Operations

Mathematical Calculations and Math Problems

Robot Planning Action

Machine Learning Training

Web Browsing Action

Download and Process Tabular Data

Data Visualization

Error Handling and Self-Debugging

API Call

Purchase a Given Product

CodeX Research: Contracts & Terms Review

- Statement of Common Agentic AI Applications and Services
- Statement of Key Use Cases, Scenarios, and Fact Patterns
- User Terms on Sites Commonly Accessed or Transacted Through by Agents
- Applicable API and Other Agentic Service Terms
- Legal Analysis, Issues, Options, and Look Ahead

UETA and ESIGN Provide Helpful Frameworks

- Electronic Agent
- Automated Transactions
- Attribution
- Security Procedures
- Electronic Signatures, Contracts, and Records

UETA and ESIGN Provide Helpful Frameworks

Electronic Agents

The term "electronic agent" means a ***computer program*** *or an electronic or other automated means* ***used independently to initiate an action or respond*** *to electronic records or performances in whole or in part* ***without review or action by an individual*** *at the time of the action or response.*

UETA and ESIGN Provide Helpful Frameworks

Automated Transactions

A contract may be formed by the ***interaction of electronic agents of the parties****, even if* ***no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements****.*

UETA Agent Transaction Error Handling

Section 10 of UETA (addressing errors) ***empowers the user to reverse transactions if the agent did not provide a means to prevent or correct the error****. This provision should be carefully understood by transactional agent providers to ensure their process flow and user interactions support and reflect adequate means to prevent or correct errors.*

UETA Agent Transaction Error Handling

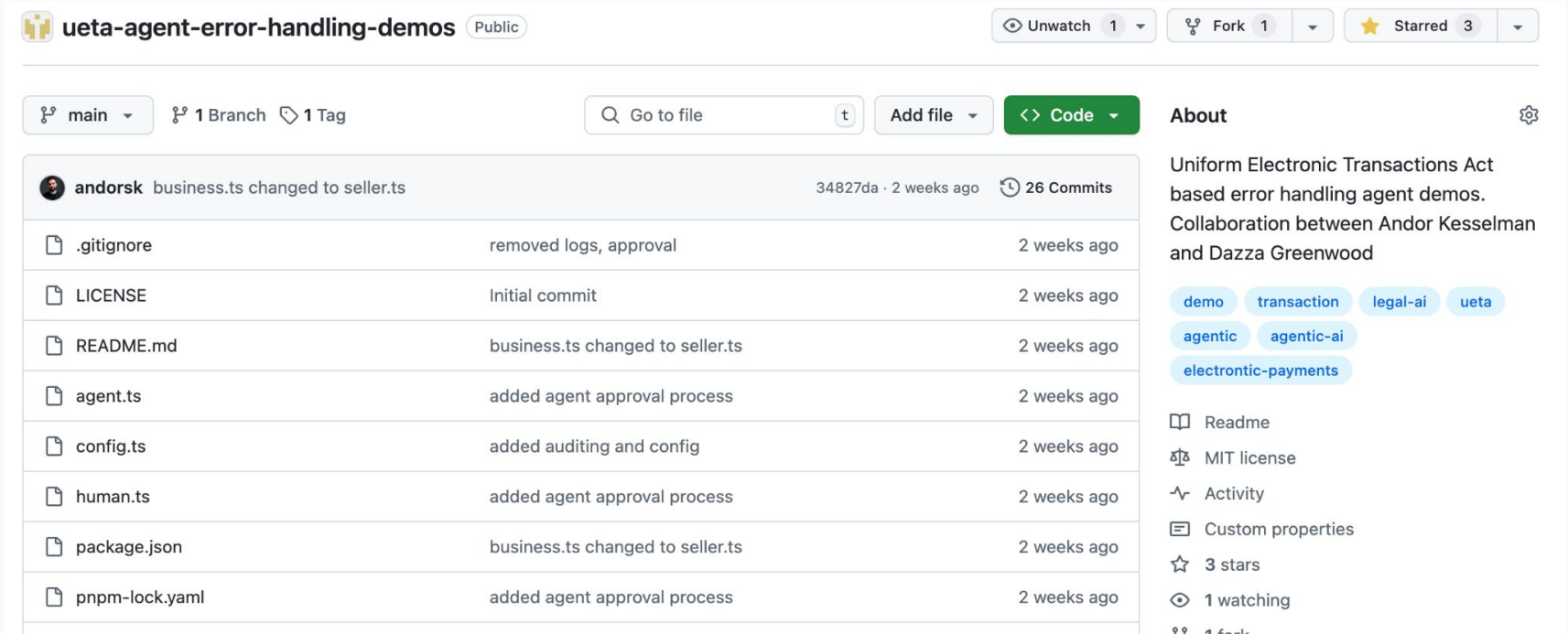
Key Relationships and Roles

	Role	Core Function	Relation to Finality
	The User	Initiates and confirms transactions	Has statutory right to reverse transactions without proper error handling
	Agent Provider	Provides the agent system to the user	Must implement error prevention/correction to achieve finality
	Third Party	Delivers goods/services	Needs protection from transaction reversal

Source: Dazza Greenwood • Get the data • Created with Datawrapper

Note: In some arrangements, the Third Party may also serve as the Agent Provider, offering an agent for users to interact with their own services.

UETA Error Handling Open Source Demo



ueta-agent-error-handling-demos Public

Unwatch 1 | Fork 1 | Starred 3

main | 1 Branch | 1 Tag | Go to file t | Add file | Code

andorsk business.ts changed to seller.ts — 34827da · 2 weeks ago — 26 Commits

.gitignore	removed logs, approval	2 weeks ago
LICENSE	Initial commit	2 weeks ago
README.md	business.ts changed to seller.ts	2 weeks ago
agent.ts	added agent approval process	2 weeks ago
config.ts	added auditing and config	2 weeks ago
human.ts	added agent approval process	2 weeks ago
package.json	business.ts changed to seller.ts	2 weeks ago
pnpm-lock.yaml	added agent approval process	2 weeks ago

About

Uniform Electronic Transactions Act based error handling agent demos. Collaboration between Andor Kesselman and Dazza Greenwood

demo | transaction | legal-ai | ueta | agentic | agentic-ai | electrontic-payments

Readme
MIT license
Activity
Custom properties
3 stars
1 watching

Newer State Law Supporting AI Agents

Innovative State Law: Wyoming Digital Identity Act and Related Statutes

- Definitions: "Personal digital identity" means the intangible digital representation of, by and for a natural person, over which he has principal authority and through which [they] intentionally communicates or acts
  - Parallel Provisions for "Organizational Digital Identity"
  - Explicit Integrations with Wyoming's Criminal Impersonation and relevant UETA provisions
- Algorithmically Managed LLCs and Non-Profits
- Coming Soon: Cryptographically verifiable identifiers for corporations & LLCs

(Some) Issues and Options

Authorize/Delegate	→	UX & Logs for Human/Agent Interface
Attribution	→	Identification of First Party
Apparent Authority	→	Communicate Actual Authority
Errors & Mistakes	→	Agreement on Use of Agents

Interested to Get Involved in this Research?

Request and invitation to the law.MIT.edu and Stanford CodeX ComputationalLaw.org Special Interest Groups on Agentic AI research at:

https://ComputationalLaw.org

Attribution: Example API Field Bootstrap

`safetyRatings[]` `object (SafetyRating)`

List of ratings for the safety of a response candidate.
There is at most one rating per category.

`citationMetadata` `object (CitationMetadata)`

Output only. Citation information for model-generated candidate.
This field may be populated with recitation information for any text included in the `content`. These are passages that are "recited" from copyrighted material in the foundational LLM's training data.

`tokenCount` `integer`

Output only. Token count for this candidate.

`groundingAttributions[]` `object (GroundingAttribution)`

Output only. Attribution information for sources that contributed to a grounded answer.
This field is populated for `GenerateAnswer` calls.

`index` `integer`

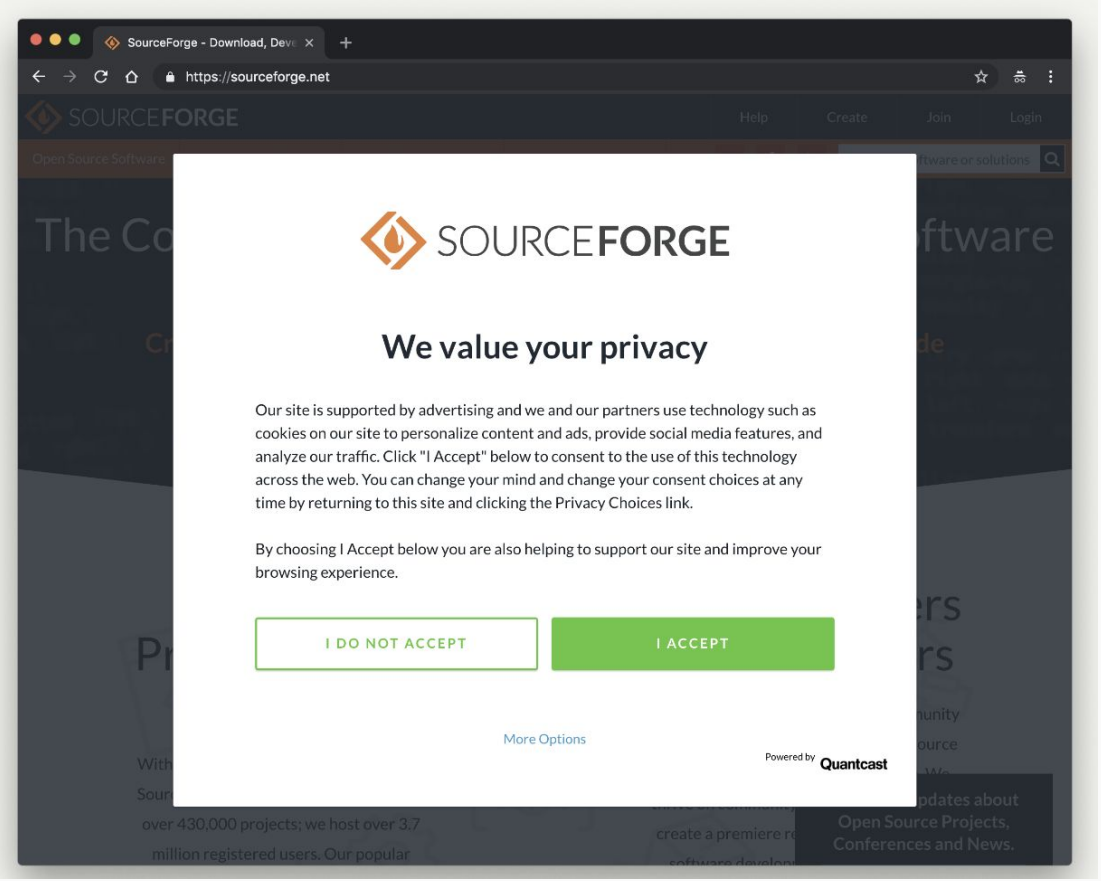
Output only. Index of the candidate in the list of response candidates.

JSON representation

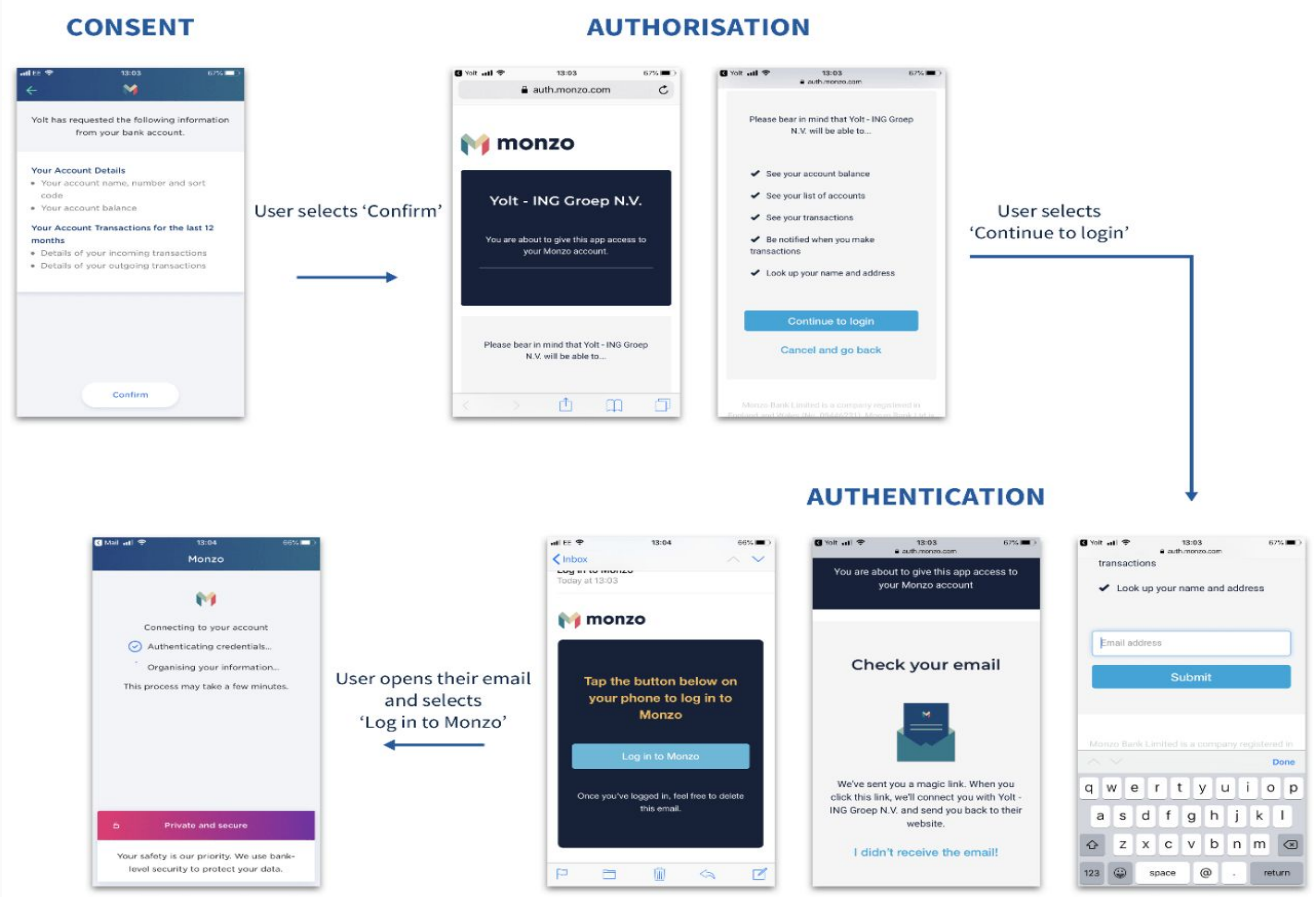
```
{
  "content": {
    object (Content)
  },
  "finishReason": enum (FinishReason),
  "safetyRatings": [
    {
      object (SafetyRating)
    }
  ],
  "citationMetadata": {
    object (CitationMetadata)
  },
  "tokenCount": integer,
  "groundingAttributions": [
    {
      object (GroundingAttribution)
    }
  ],
  "index": integer
}
```

Google Gemini API Attribution Field

Consent and Authorization Best Practices



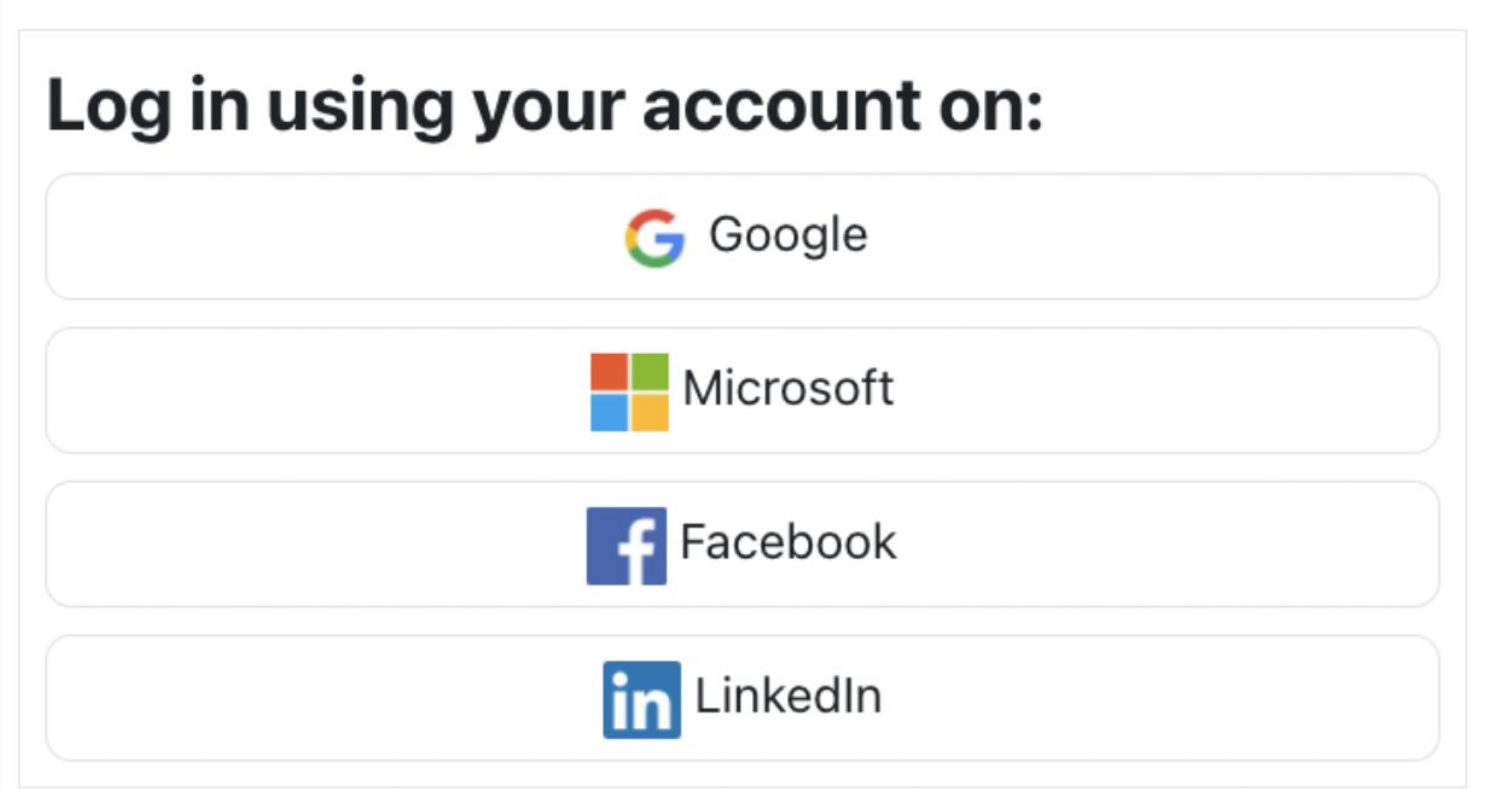
Consent and Authorization UI/UX Good Practices



Consent & Authorization Tech for Agent Flows

Oauth 2 and
OpenID Connect

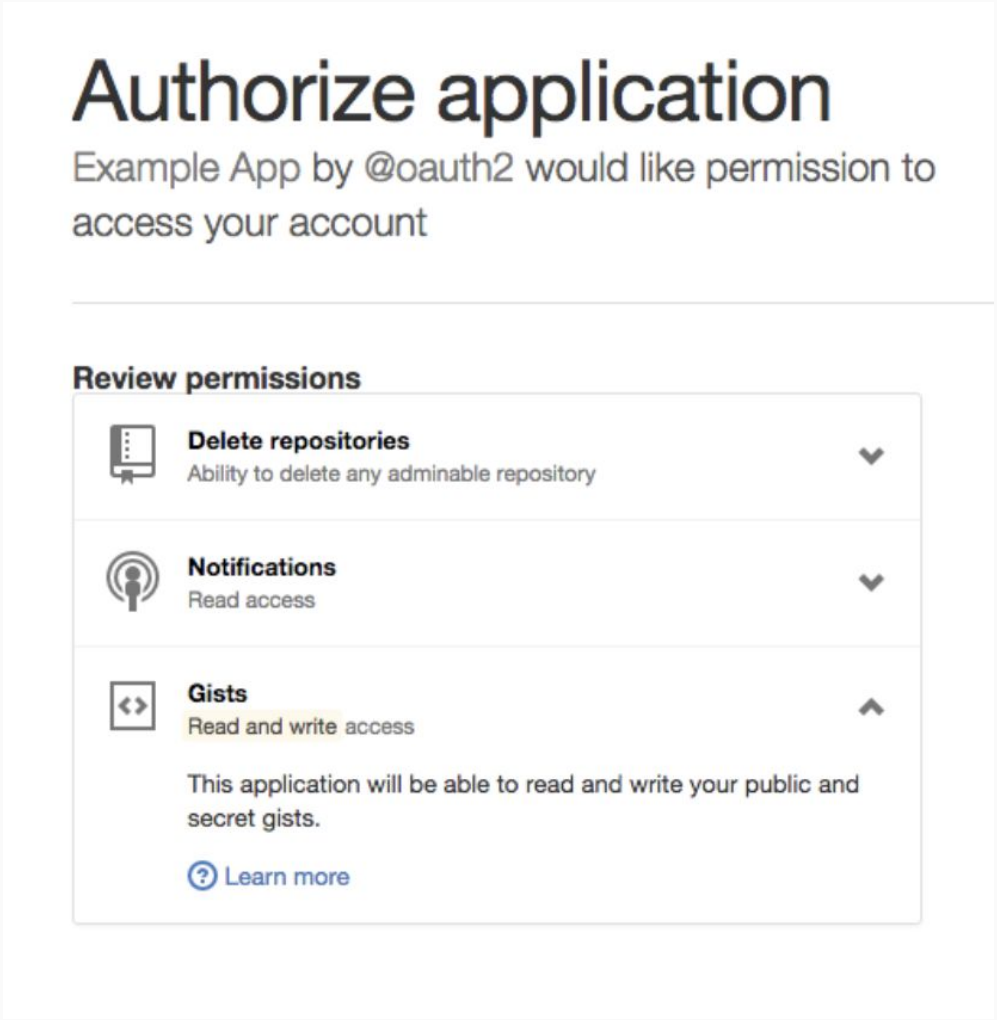
...You know it best for login



Consent and Authorization

Potentially Well Suited Technical Approaches:

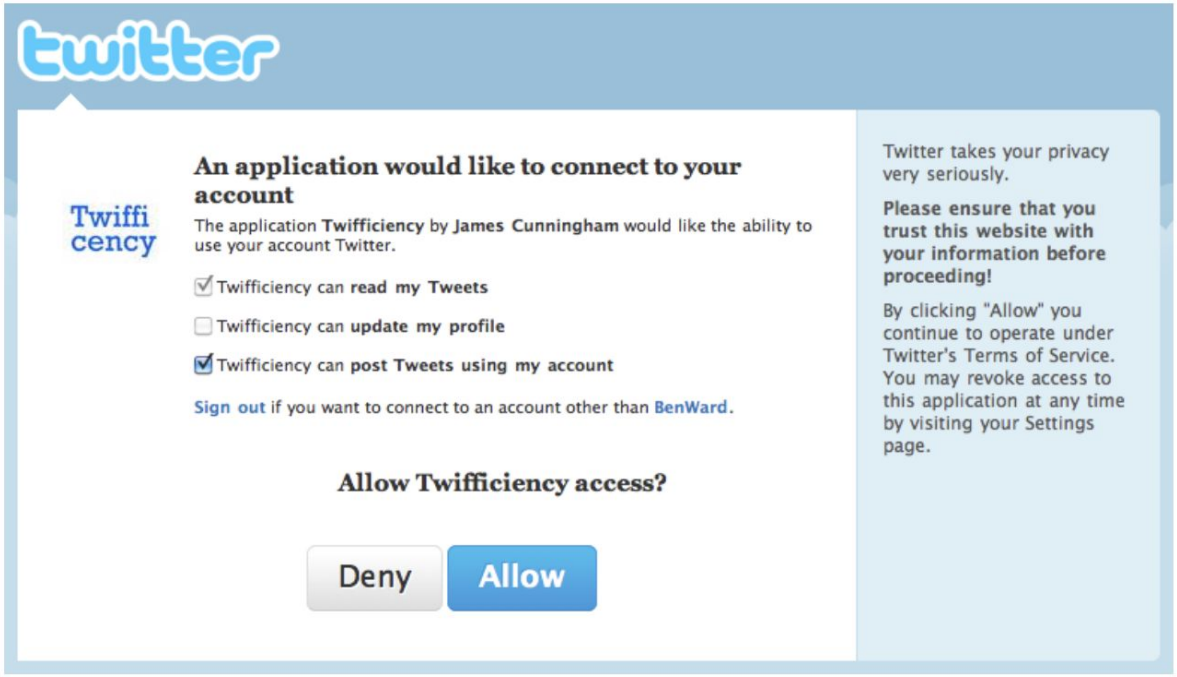
Oauth 2 & OpenID Connect works for many scope of authority beyond login



Consent and Authorization

Potentially Well Suited Technical Approaches:

Authorizations can be fine-grained and clearly delegated



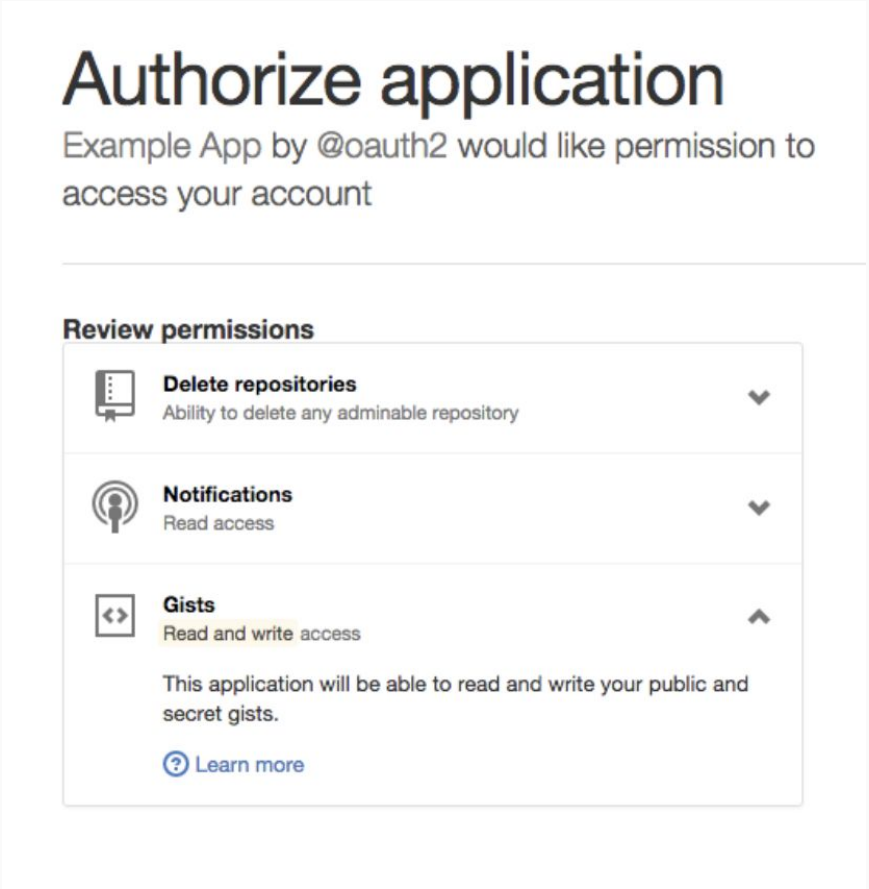
- **Passkeys use unique cryptographic key pairs** for each account: private key stored securely on your device, public key used for authentication
- **Enable biometric login** with Face ID or Touch ID, eliminating the need for passwords
- **Work seamlessly across devices** and are gaining support from major apps, platforms, and online services

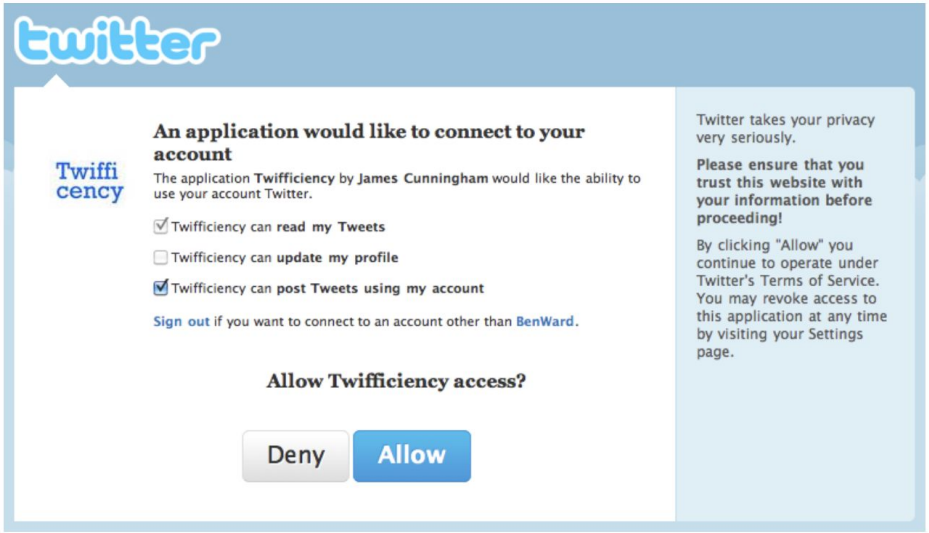
Consent and Authorization

Potentially Well Suited Technical Approaches:

Passkey in Apple Ecosystem

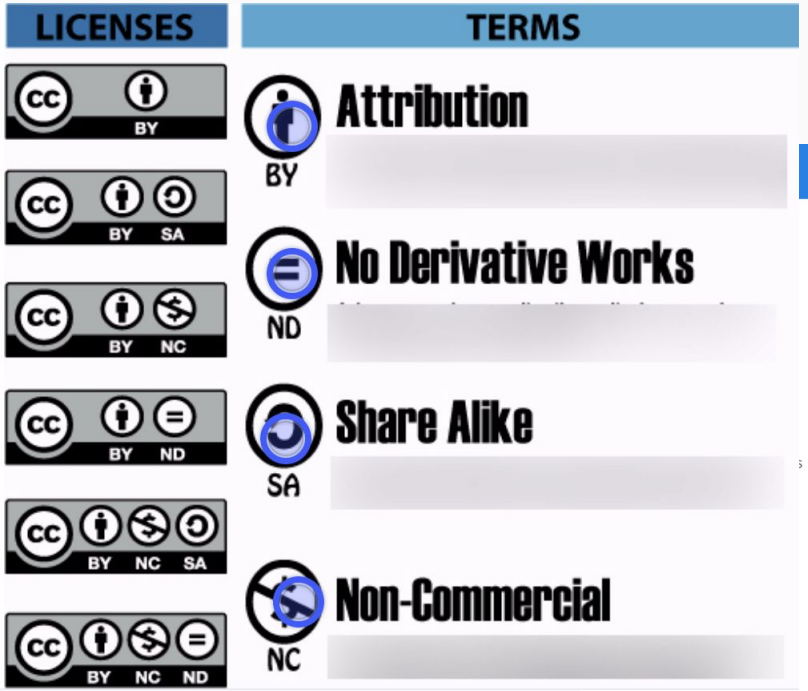
Consent and Authorization Good Tech Examples

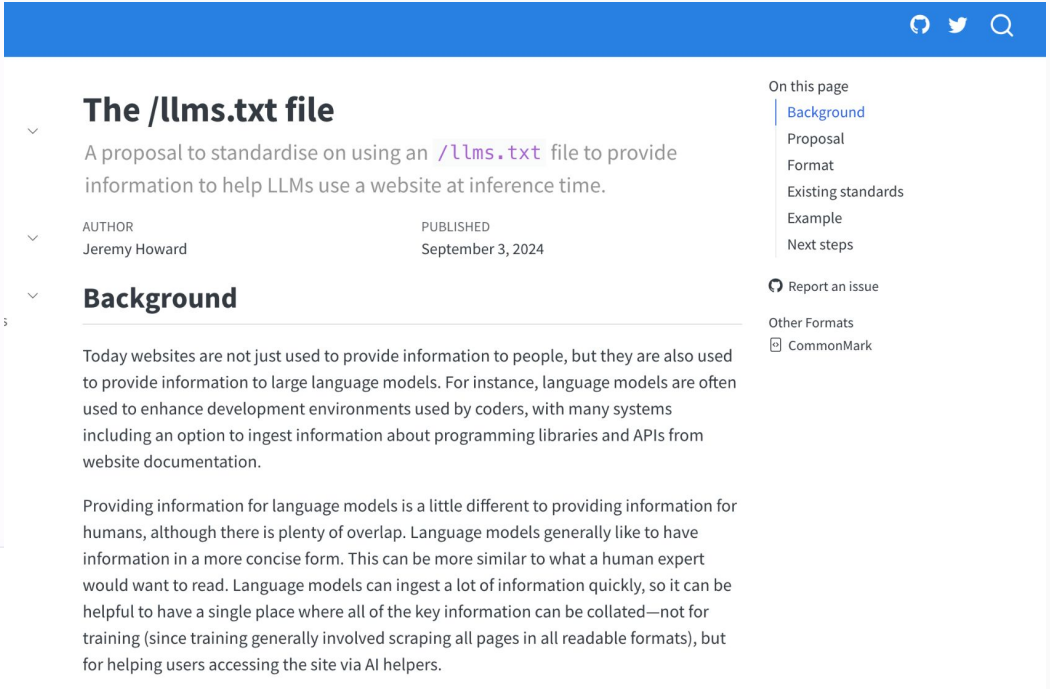




Agreement on Agentic AI: One-Way Terms

Creative Commons & llms.txt





The /llms.txt file

A proposal to standardise on using an `/llms.txt` file to provide information to help LLMs use a website at inference time.

AUTHOR
Jeremy Howard

PUBLISHED
September 3, 2024

Background

Today websites are not just used to provide information to people, but they are also used to provide information to large language models. For instance, language models are often used to enhance development environments used by coders, with many systems including an option to ingest information about programming libraries and APIs from website documentation.

Providing information for language models is a little different to providing information for humans, although there is plenty of overlap. Language models generally like to have information in a more concise form. This can be more similar to what a human expert would want to read. Language models can ingest a lot of information quickly, so it can be helpful to have a single place where all of the key information can be collated—not for training (since training generally involved scraping all pages in all readable formats), but for helping users accessing the site via AI helpers.

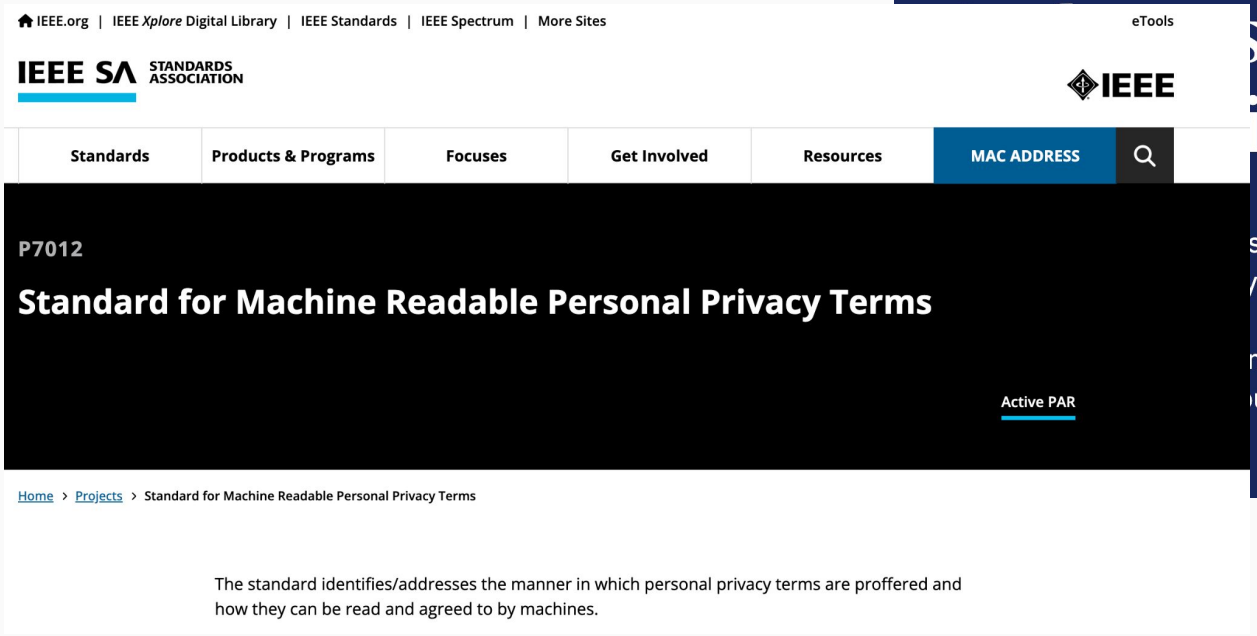
On this page
Background
Proposal
Format
Existing standards
Example
Next steps

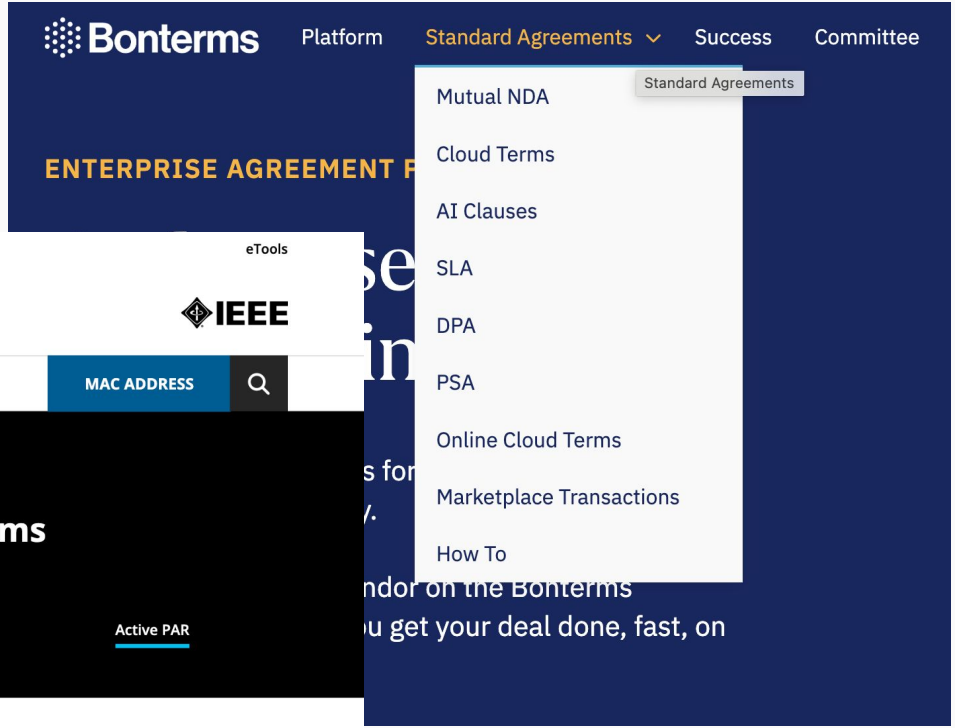
Report an issue

Other Formats
CommonMark

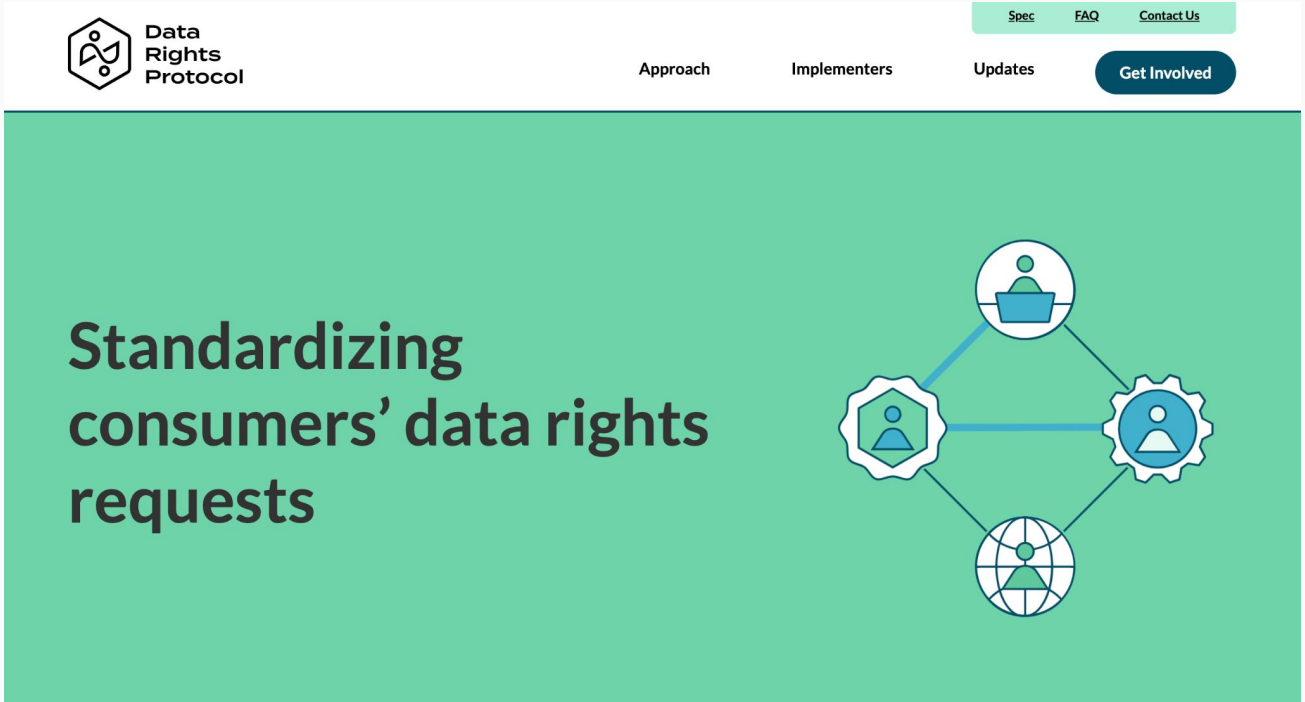
Agreement on Agentic AI: Two-Way Terms

P7012 & Bon Terms





Personal Data & Individual/Consumer LLM Agents



Interested to Get Involved in this Research?

Request and invitation to the law.MIT.edu and Stanford CodeX ComputationalLaw.org Special Interest Groups on Agentic AI research at:

https://ComputationalLaw.org

Thank you!