UNIVERSITY OF CALIFORNIA

UC LEGAL - OFFICE OF THE GENERAL COUNSEL
Legal Alert: *Artificial Intelligence Tools*

March 2024

Q: What guardrails should UC Units utilize when using artificial intelligence (AI) tools?[1]

A: UC Units should be mindful of the data provided to AI tools, including generative AI, the output generated by such tools, how UC uses and relies on the outputs or predictions of an AI tool, and their terms of use. Any use of commercial AI products should be subject to prior review and approval of terms by procurement, privacy, security, risk, and legal counsel, as appropriate.

Background

This Alert is geared solely towards *legal* concerns with respect to AI tools, such as those that involve generative AI,[2] automated decision systems (ADS),[3] or machine learning.[4]

The use of such AI-enabled tools raises legal, compliance, and ethical questions to consider.[5] This Alert offers the following legal-focused guardrails for use of these tools. Most important, though AI, and in particular, generative AI, has propelled into public view, it is nevertheless a tool that calls for the same type of analysis as any other third-party service or product. Indeed, like any tool utilized by UC, whether for education, research, health care, or operational purposes, AI tools and their terms of use are subject to all UC policies regarding third parties and their access to UC data, such as those relating to procurement, research, privacy, data security, accessibility and employee, faculty, and student conduct.

[1] AI broadly encompasses technology that aims to reproduce or exceed abilities in computational systems that would require human-like thinking to perform a wide range of tasks, from simple to sophisticated. UC Presidential Working Group on Artificial Intelligence, Responsible Artificial Intelligence Recommendations to Guide the University of California's Artificial Intelligence Strategy (October 2021) (UC AI Report).

[2] "Generative AI" broadly encompasses artificial intelligence technology that can be used to produce new text, images, video, audio, code, or synthetic data. Such AI tools generate responses based on user prompts or user data, as well as data scraped from public websites. They fine-tune themselves to understand and interpret user inquiries, then generate relevant responses. Tools such as ChatGPT are versatile, able to write computer programs, compose music and essays, play games, and simulate chat rooms.

[3] ADS can be defined as "a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision or facilitates human decision making." UC AI Report.

[4] ML is a method of data analysis that automates analytical model building. It is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns, and make decisions with minimal human intervention. UC AI Report.

[5] For discussion of some of these ethical considerations by UC, refer to the UC AI Report.

1. Generative AI Tools and Confidential Information of UC and Third Parties, Privileged Information, and Personal Information

Unless specific precautions are taken, any content that is provided to generative AI tools can be saved and reused by the company offering the tool (e.g., OpenAI for ChatGPT) and their affiliates. Providing data to a generative AI tool requires the same analysis as when UC provides data to any service vendor, research partner, or other third party. Therefore, unless Units enter into properly negotiated agreements with these companies, which would include privacy, confidentiality, security, accessibility and intellectual property terms consistent with UC policy and appropriate for the types of information at issue, Units are prohibited from providing any information that could be construed as confidential information of UC, or confidential information of a third party. Such disclosure could cause UC to be in violation of statutory or contractual requirements.

Confidential information of UC or of third parties, including information that may be protected by a privilege, such as attorney-client privileged information, or psychotherapist-patient information, also may not be provided to generative AI tools. UC employees do not have the authority to disclose attorney-client privileged information of UC to third parties.

Similarly, without proper vetting of agreements with generative AI companies and their data security and use policies consistent with UC's Electronic Information Security Policy (IS-3) and local data security policies, Units are prohibited from providing generative AI companies and tools with personal information, including but not limited to, the financial or medical information of UC's employees, students, and patients. Such disclosure (even if the data is de-identified) could run afoul of underlying laws protecting the data, such as the Health Insurance Portability and Accountability Act (HIPAA), the California Confidentiality of Medical Information Act (CMIA), and the California Information Practices Act (IPA). Not only would sharing this information be a privacy violation, but this data could also be exposed by a data breach. Indeed, in March 2023, a bug leaked ChatGPT users' "first and last name, email address, payment address, the last four digits (only) of a credit card number, and credit card expiration date". https://openai.com/blog/march-20-chatgpt-outage. Breaches such as these could subject UC to reporting obligations and penalties under state and federal breach notification statutes.

2. Output of AI Tools and UC's Reliance on Them

Output generated by generative AI tools, including chatbots, may not always be correct, and could also infringe on the intellectual property rights of others. If UC has not negotiated contract terms in accordance with its policies and practices, there are likely few protections in place. UC should have the opportunity to directly negotiate and impose obligations on the vendors to defend and indemnify UC against claims brought by third parties. Some AI companies have also recognized that their tools sometimes exhibit biased behavior. See more about the limitations of ChatGPT here.

Data sets used to train AI, and the resulting models, can also contain illegal content, such as child sexual abuse material. Of course, it is important to avoid storing illegal content on UC systems, even inadvertently.[6]

[6] D. Thief, Investigation Finds AI Image Generation Models Trained on Child Abuse. Stanford University, December 20, 2023.

Moreover, several agencies have issued guidance, alerting organizations such as UC about the use of AI tools and potential concerns they raise with respect to output and actions taken based on such output:

- U.S. Equal Employment Opportunity Commission (EEOC): If use of an algorithmic decision-making tool has an adverse impact on individuals of a particular race, color, religion, sex, or national origin, the use of the tool will violate Title VII unless the employer can show that such use is "job related and consistent with business necessity."[7]
- U.S. Department of Education (DOE): Educators and institutions must consider questions such as how to protect student privacy and data (in both the data inputted and output generated), how to evaluate the impact of using AI for learning on all students, and to what extent educators are able to exercise voice and decision-making to improve equity, reduce bias, and increase cultural responsiveness in the use of AI-enabled tools.[8]
- U.S. Department of Health & Human Services (HHS): AI applications can result in discriminatory outcomes that negatively impact individuals protected by the Civil Rights Act, the Rehabilitation Act, the Age Discrimination Act, and Section 1557 of the Patient Protection and Affordable Care Act, and HHS has the authority to enforce these statutes in the context of AI. The Health Information Technology for Economic and Clinical Health (HITECH) Act indirectly authorizes HHS to regulate AI applications by establishing requirements for the safeguarding and notification of a breach of protected health information which may occur through use of an AI application by a HIPAA-regulated entity.[9]
- U.S. Federal Trade Commission (FTC): The FTC has expressed concerns both about the use of AI to deceive customers and the way AI systems are trained. Consumers may be harmed if there is a lack of transparency about content created by AI tools. Additionally, the FTC has warned that, in training AI systems, the use of third-party copyrighted works (without the consent of third parties) may run afoul of FTC consumer protections law, in particular, clauses that prevent "unfair methods of competition."[10]

Note, the above is a non-exhaustive list. There are also several states that are regulating use of AI.

It is important for UC to ask suppliers providing a tool that uses AI to the University, where UC relies on that tool to take an action related to a student, employee, patient, research subject, or security of a UC resource, about the sources of datasets used to train their AI models, and to understand how the supplier evaluates these datasets for bias and inaccuracy. Indemnity and limitation of liability provisions relating to such AI tools should also be carefully reviewed to ensure that the Supplier has appropriate responsibility to UC for the outputs its tools generate.

3. Free-to-Use Generative AI Terms

Generative AI services have terms of use and/or privacy policies that should be reviewed, as they may automatically apply if the service is used. Acceptance of such terms as written could expose UC to unacceptable and costly risks, including, but not limited to, liability for third-party acts or omissions,

[7] EEOC. "Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964" (accessed August 1, 2023). Title VII generally prohibits employment discrimination based on race, color, religion, sex, or national origin.

[8] DOE. Artificial Intelligence and the Future of Teaching and Learning. May 2023.

[9] HHS. Trustworthy AI Playbook. September 2021.

[10] FTC. "Consumers Are Voicing Concerns About AI." October 2023.

privacy law violations, and liability for infringement. Work with local procurement officers prior to finalizing any transactions to include agreement terms that comply with UC policies.[11]

4. Location Risk Assessments and Review

Whether for internal UC business, education, research, or other purposes, use of free-to-use and paid AI products must undergo location-based risk assessments by information security, with participation from privacy officers, and legal counsel, as appropriate, just like any other product or service that would be utilized by UC. Procurement offices should also review and negotiate problematic terms such as insurance, indemnification, and limitations of liability with appropriate input from risk, privacy, security, and other units. Given the potential use of these products to access regulated data (e.g., scanning student essays or other FERPA-protected records for plagiarism, or parsing patient health information to facilitate access to care and improve outcomes), such contracts must include an Appendix Data Security, and, where PHI is involved, an Appendix - Business Associate Agreement. Locations should also conduct an equity or non-discrimination assessment[12] of the tools to be used, in consideration of recent enforcement action at both the federal and state level related to AI bias.

Contact: UC Legal AI Task Force, Legal Support Working Group

Jennifer Achtert, Principal Counsel, UCOP
Leonid Balaban, Sr. e-Discovery Specialist, UCOP
Jessica Jung, Principal Counsel, UCOP
Hillary Kalay, Senior Principal Counsel, UCOP
Jonathan Lee, Assistant Counsel, UCSD Health
Kyhm Penfil, Campus Counsel, UC Irvine
Angus MacDonald, Managing Counsel, UCOP
Sajjad Matin, Principal Counsel, UCOP
Jerome Mayer-Cantú, Principal Counsel, UCOP
Joshua Meltzer, Principal Counsel, UCOP
Sarah Suskauer, Principal Counsel, UCSD Health
Mark Wilson, Principal Counsel, UCOP
Michelle Wong, Principal Counsel, LBNL
Tammi Wong, Principal Counsel, UCOP
Darnele Wright, Deputy General Counsel, UCOP

[11] For example, users of ChatGPT's free version are automatically deemed to have agreed to its Terms of Use and Privacy Policy, which are subject to change. These terms include:

- Restrictions on use and distribution of ChatGPT content;
- The right for OpenAI to use content provided to it to help develop and improve its Services;
- An obligation to defend, indemnify, and hold OpenAI and its affiliates and personnel harmless from and against all claims "arising or relating to your use of the Services." Note that this violates Standing Order 100.4(dd)(9), which could subject UC to third-party claims.
- A limitation of OpenAI's liability, with aggregate liability not exceeding the greater of the amount paid to use ChatGPT, or $100; and
- Unless this form is completed, within 30 days of using ChatGPT any dispute with OpenAI over the use of ChatGPT is subject to final and binding arbitration. The arbitration terms are here.

[12] Equity assessments are systematic examinations of available data and expert input on how various groups – especially those facing inequalities or disparities – are or likely will be affected by a policy, program, or process. U.S. Dep't. Of Health & Human Servs., Conducting Intensive Equity Assessments of Existing Programs, Policies, and Processes. September 2022. See also Olyaeemanesh A, Takian A, Mostafavi H, Mobinizadeh M, Bakhtiari A, Yaftian F, Vosoogh-Moghaddam A, Mohamadi E. Health Equity Impact Assessment (HEIA) reporting tool: developing a checklist for policymakers. Int J Equity Health. 2023 Nov 18;22(1):241. doi: 10.1186/s12939-023-02031-0. PMID: 37980523; PMCID: PMC10657117.