With privacy being a major concern among the public and a top risk for both private and government entities, University Compliance Services distributes the Privacy Matters @ WWU newsletter to highlight important privacy developments and to provide a centralized platform where University Privacy Owners and stakeholders can connect on privacy topics in an effort to strengthen Western’s Privacy Program.

In this Newsletter

- Privacy Risks Associated with Artificial Intelligence
- Current Regulatory Activity to Mitigate the Risks of Artificial Intelligence

Privacy Risks Associated with Artificial Intelligence

As artificial intelligence ("AI") technology rapidly advances so do the risks.

Commonly understood risks of AI are:

- Discriminatory or biased outcomes when systems using AI algorithms replace humans in making decisions, such as in hiring, admissions, financial aid, or loan determinations.

- Student cheating when AI is used to solve homework or test problems or to create essays.

But what are the privacy risks of AI?

AI presents several privacy risks and concerns, including:
• **Unauthorized sharing of data:** Generative AI systems, such as ChatGPT can be used to create tables and graphs by copying and pasting data into the system.

For example, employee data can be pasted into the system to create a compensation or leave chart for a presentation. If personally identifiable information is included in the data input, that data is now embedded in and accessible through ChatGPT by other users.

• **Data breaches:** AI systems, such as the university’s third-party systems, often rely on vast amounts of data to train and operate effectively. Data used for this purpose may contain confidential personal information and, if not handled properly, it can lead to privacy breaches.

• **Manipulation of media:** Generative AI systems can create, edit, modify and read from a wide range of media files. This poses a risk of significant harm to others whose personal photos posted in social media are used to create explicit photos and later posted.

• **Surveillance:** AI powered surveillance systems can track and analyze individuals’ behavior (biometric data), leading to concerns about invasion of privacy, particularly in public spaces.

• **Profiling and targeting advertising:** AI algorithms can analyze user data to create detailed profiles, enabling targeted advertising. While this can improve ad relevance, it also raises concerns about manipulation and exploitation of personal information.

• **Inference of sensitive information:** AI systems can sometimes infer sensitive information about individuals from seemingly innocuous data, posing risks to privacy even when explicit information is not provided.

• **Cross-referencing data:** AI systems can aggregate data from multiple sources to create comprehensive profiles of individuals, increasing the risk of privacy breaches and unauthorized access.

---

**Current Regulatory Activity to Mitigate the Risks of Artificial Intelligence**

1. **Governor Inslee’s Executive Order 24-01:**

The executive order directs the development of a number of initiatives led by WaTech and other agencies to create procurement guidelines, training plans for state workers, reports on AI initiatives and frameworks to ensure accountability and assess risks. There also will be guidelines focusing on the impact of AI on vulnerable communities and the state workforce.

Deliverables, deadlines, and who is involved can be found in this high-level overview. WaTech invites individuals interested in getting involved in any of the initiatives to reach out to the state Privacy Officer at privacy@watech.wa.gov.
2. Interim Guidelines for Responsible Use of AI in Washington State Government

These guidelines serve as an initial framework for the responsible and ethical use of generative AI technologies within the Washington state government.

3. Washington State E2SSB 5838 (2024): Establishing an Artificial Intelligence Taskforce

This bill creates a task force to:
- Assess current uses and trends by private and public sector entities, and
- Make recommendations to the Legislature regarding standards for the use and regulation of AI.


- Expands certain criminal offenses prohibiting the dealing in, sending or bringing into the state of, possessing of, or viewing of, depictions of a minor engaged in sexually explicit conduct to include circumstances involving fabricated depictions of an identifiable minor.
- Establishes the offense of Disclosing Fabricated Intimate Images, which a person commits if the person discloses a fabricated intimate image of another person and knows or should know that the depicted person has not consented to disclosure, and that disclosure would cause harm to the depicted person.
- Establishes a civil cause of action for the nonconsensual, intentional disclosure or threatened disclosure of a fabricated intimate image.

Please send in your newsletter content comments, suggestions, and questions to compliance.matters@wwu.edu