



Microsoft Copilot Opportunities & Risks

Jeff Jones – Director of Digital Work Experience

Enterprise Solutions

Information Services - University of Oregon





Communication and Governance

- Communicate these opportunities & risks to stakeholders
 - Chiefs of Staff
 - Records Stewards
 - Email Calendaring & Collaboration Service Advisory Board
 - Summer Teaching Institute
 - Administrative Technologies Domain Committee
 - Etc.
- AI Leadership Council
 - Governance Committee
 - Important decisions need to be made
 - What is our AI strategy?

Chat GPT

- **Large Language Model (LLM)**
 - Trained on vast amounts of data, allowing it to generate natural language responses to a variety of prompts.
- **GPT-4 versus GPT-3.5**
 - Bar Exam
 - GPT-3.5: 10th percentile
 - GPT-4: 90th percentile
- **GPT-4**
 - Cost: \$20 per user per month
 - Compliance Concerns:
 - Your prompts are used to train the model
 - Your information is not private!
 - **Example:** Paste a patient's medical chart into ChatGPT



Microsoft & OpenAI

- **"Microsoft Invests \$10 Billion in ChatGPT Maker OpenAI"**
 - *Bass, D. (2023, January 23). Microsoft Makes Multibillion-Dollar Investment in OpenAI. Bloomberg.*



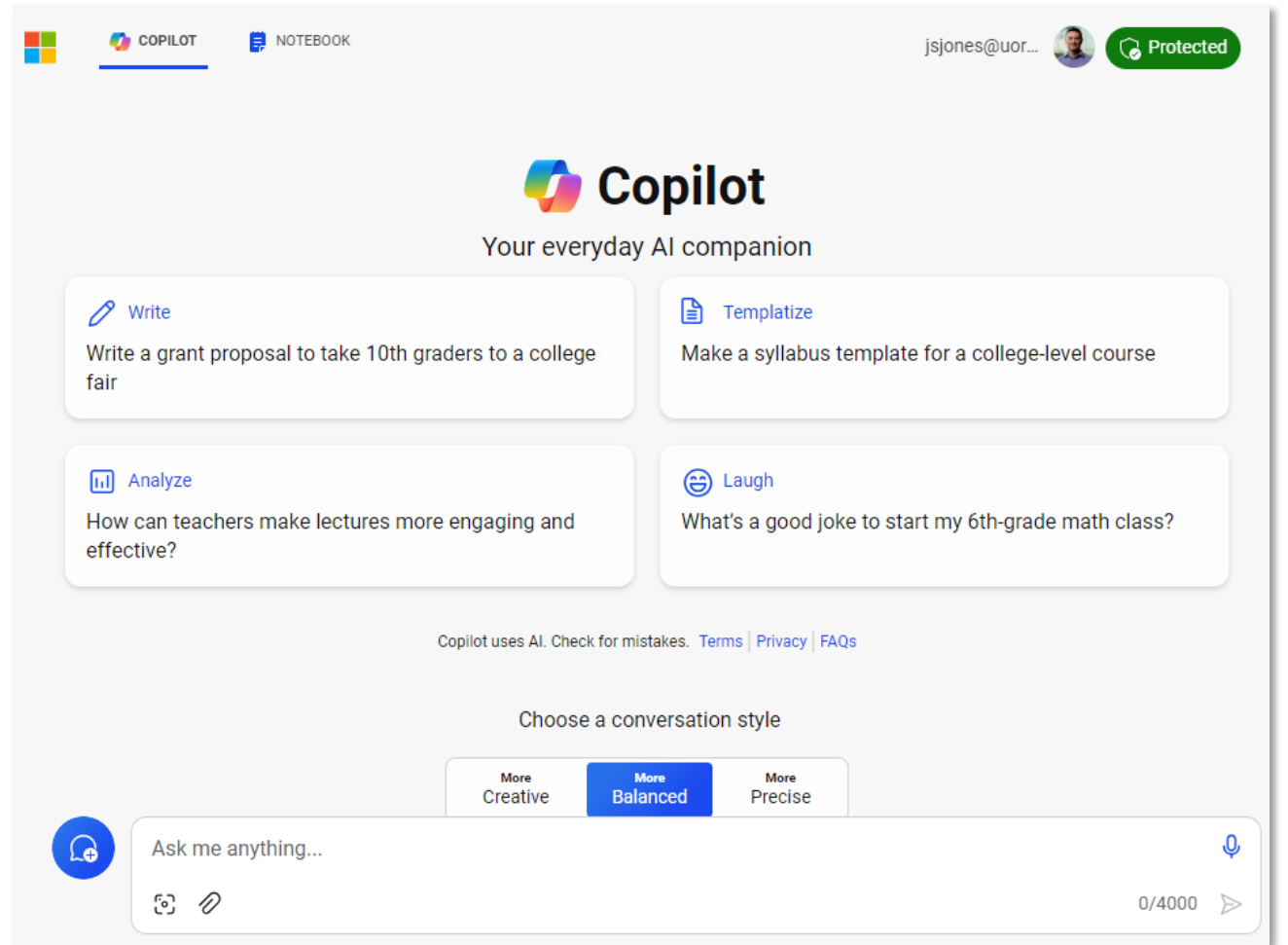
Microsoft Product Offerings

- **Microsoft Copilot (for the web)**
 - Formerly known as Bing Enterprise chat
- **Copilot for Microsoft 365**
 - Integrates with Word, Excel, PowerPoint, Outlook & Teams.
- **Copilot Studio**
 - An AI platform allows you to create and customize copilots
- **GitHub Copilot**
 - An AI-powered coding assistant
- **Microsoft Copilot for Security**

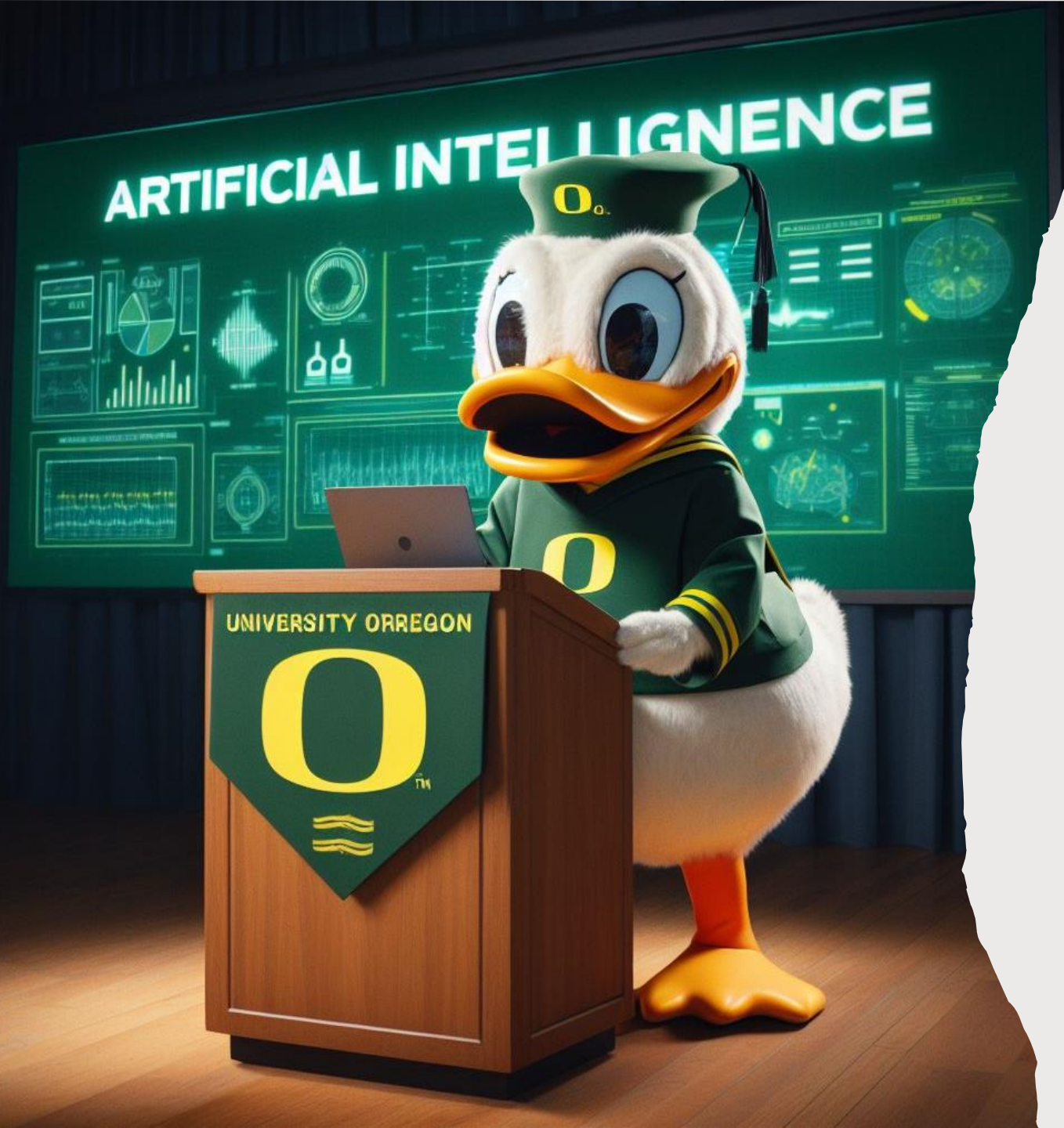


Microsoft Copilot (for the web)

- You already have access!
- Login with your duckid
 - <http://copilot.microsoft.com>
- Install the app
 - Apple
 - Android



The screenshot shows the Microsoft Copilot web interface. At the top, there are navigation elements including the Windows logo, 'COPILOT', and 'NOTEBOOK'. On the right, the user's email 'jsjones@uor...' is displayed next to a profile picture and a 'Protected' status indicator. The main heading is 'Copilot' with the tagline 'Your everyday AI companion'. Below this, there are four interactive cards: 'Write' (with a pencil icon) with the prompt 'Write a grant proposal to take 10th graders to a college fair'; 'Templatize' (with a document icon) with the prompt 'Make a syllabus template for a college-level course'; 'Analyze' (with a bar chart icon) with the prompt 'How can teachers make lectures more engaging and effective?'; and 'Laugh' (with a smiley face icon) with the prompt 'What's a good joke to start my 6th-grade math class?'. Below the cards, a disclaimer states 'Copilot uses AI. Check for mistakes.' followed by links for 'Terms', 'Privacy', and 'FAQs'. A section titled 'Choose a conversation style' features three buttons: 'More Creative', 'More Balanced' (which is selected and highlighted in blue), and 'More Precise'. At the bottom, there is a text input field with the placeholder 'Ask me anything...', a microphone icon, and a character count '0/4000' with a send button.



Microsoft Copilot

(for the web)

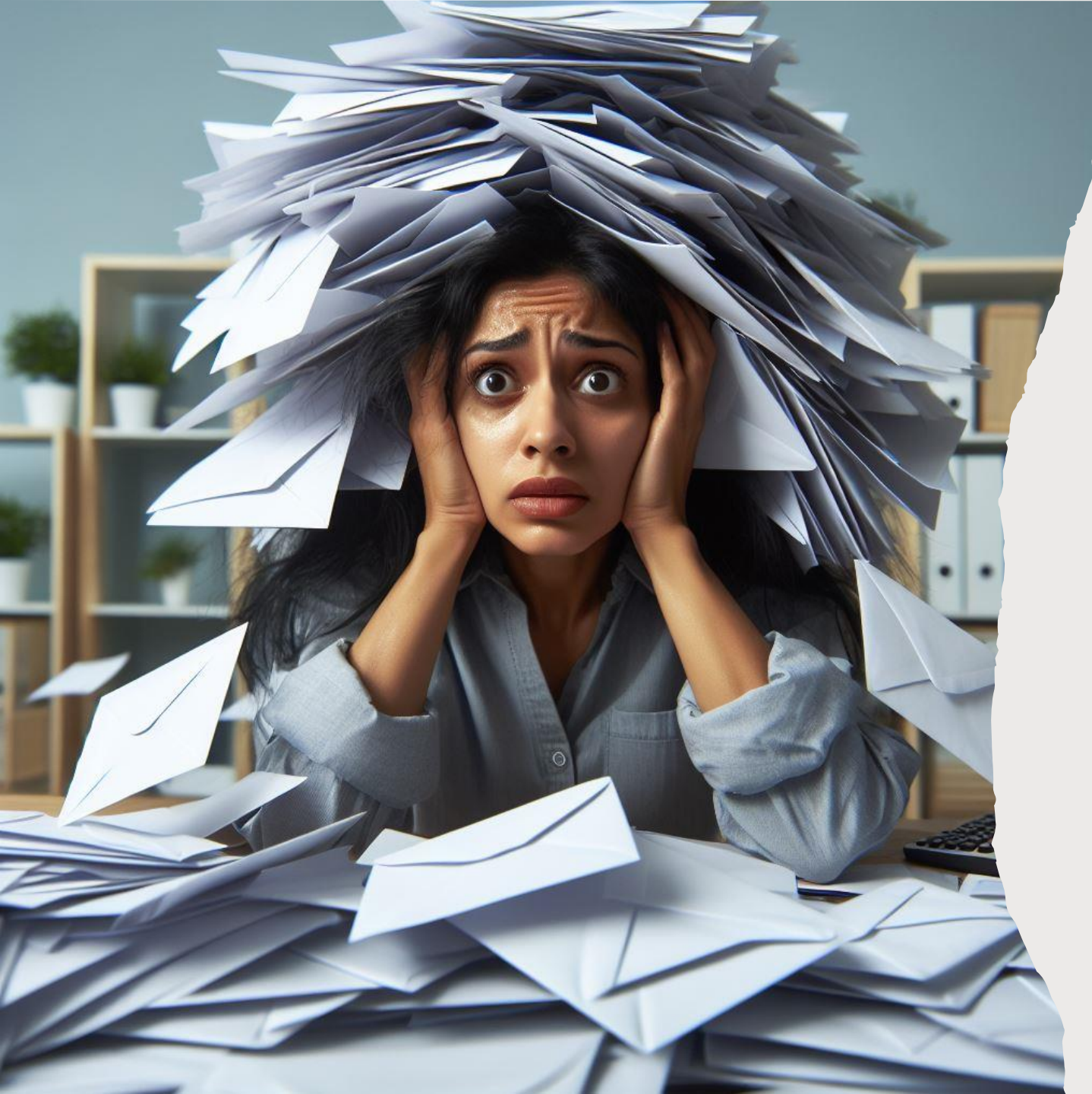
- **Text Generator: Via ChatGPT-4 Turbo!**
 - **Prompt:** "Write a short rhyme explaining what ChatGPT can do for someone unfamiliar with it"
 - **Output:** "ChatGPT, at your command, A digital friend, both clever and grand. Ask me questions, seek advice, I'll conjure answers, precise and nice."
- **Image Generator: Via DALL-E 3**
 - **Prompt:** "Create an image of the University of Oregon duck mascot standing at a podium delivering a presentation on artificial intelligence"
- **Who is Licensed?**
 - UO Staff & Faculty: Available now!
 - Students – Available now!
- **Is it Secure?**
 - **Yes, if you login with your UO credentials!**
 - It is **NOT** trained on UO's data.
 - It is **NOT** sharing UO's data.
 - [Copilot Privacy and Protections | Microsoft Learn](#)

Copilot for Microsoft 365



- **What Is It?**
 - ChatGPT integrated into Word, Excel, PowerPoint, Outlook & Teams
- **Who is Licensed?**
 - A small pilot group
 - \$30 per user per month
- **Leverages UO's enterprise data**
 - Open AI's Chat-GPT does not have access to UO data





Outlook – Copilot for M365

- You just returned from vacation to **500 unread emails** & **50 unread Teams messages**
- **Copilot:** *“Please **summarize** my unread emails and Teams messages and tell me if I missed anything important”*

Microsoft Te

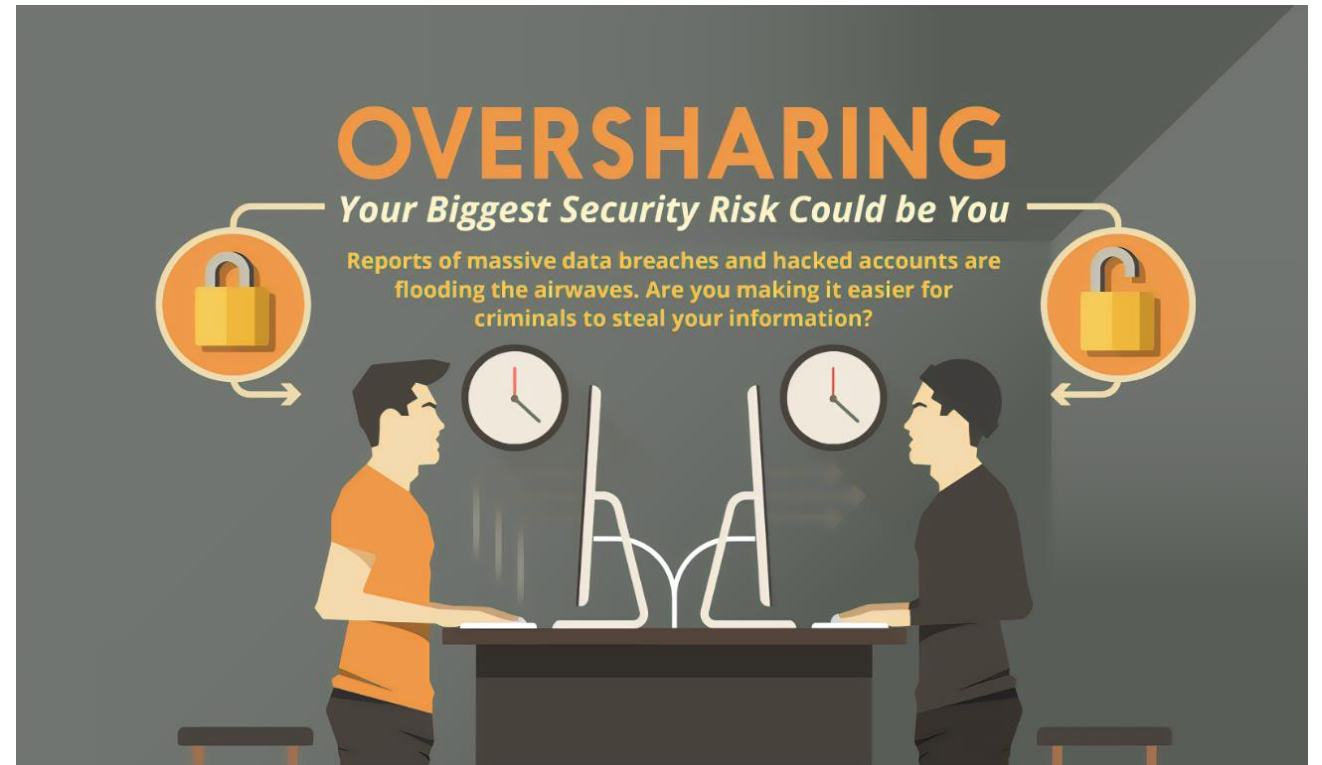


Microsoft Teams - Copilot for M365

- **Meeting Preparation**
 - *"Copilot please look through my emails, Teams chats and meeting minutes and help me prepare for my 9:30 meeting with Susan"*
- **Meeting Minutes**
 - *"Copilot please summarize today's meeting and send out the minutes to all attendees"*
 - *"Please also draft a project plan based on what you heard in our discussion."*

Risks: Oversharing

- [In Massive Security Oversight, Thousands of Private University Documents Left Vulnerable](#)
 - Harvard Crimson - October 12, 2021
- [IT Oversight Left Thousands of Harvard Internal Files Vulnerable — Again](#)
 - Harvard Crimson – April 12, 2022





Collaboration Pre-2010's

- Tools
 - Network File Servers & VPN
- IT controlled access to data
- **Example:**
 - Collaborating on a spreadsheet external to the org required:
 - Email it
 - Work with IT:
 - Credentials
 - VPN
 - File Share Permissions



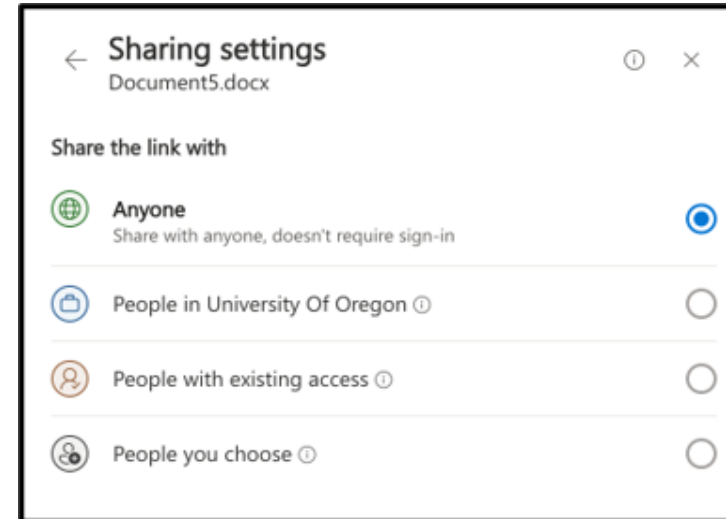
Cloud Era Post 2010

Easy Button

- No IT involvement
- Collaborate in just a few clicks
- Users have full control of their data

Oversharing!

- **IT Oversight** Left Thousands of Harvard Internal Files Vulnerable — **Again!!!**
 - Harvard Crimson
- **UO Examples**
 - **Professor:** Shared class roster with all of campus
 - **Enrollment:** Shared spreadsheet with data for all incoming freshman with all of campus





Oversharing

- Copilot for M365 has access to UO's data
 - **Copilot will not grant access to others**
 - **It will adhere to the access controls put in place by the user**
- Oversharing can have **disastrous** consequences
 - Examples:
 - **Stanford** – 300 user pilot – Board of Directors – info leak
 - **Teams Meetings** – AI could be listening

What should we not do?

- **We can't ignore AI**
- Our users **will use** these tools whether we offer them or not
 - Examples: Slack, Box, Google, etc.



What should we do?

- Train our users
 - Information Security Training is more important than ever!
 - Evaluate the technology with proper guardrails
- Remind folks to audit their shares:
 - [Article - Checking Your File Sharing ... \(uoregon.edu\)](#)



Questions or
Comments?

