PROFESSIONAL ETHICS IN AN AI WORLD

STEPHEN W. MINDER, CPA, CIA, CISA, CFE

CEO, YCN GROUP, LLC

ETHICS

Doing the **RIGHT** thing for the **RIGHT** reason(s) within the **RIGHT** timeframe(s).

HOW HAS AI CHANGED OUR PERCEPTION OF:

- THE RIGHT THING
- THE RIGHT REASON
- THE RIGHT TIMEFRAME

POTENTIAL ETHICAL CONUNDRUMS

- THE WORK WE DO
- THE WORK DONE THAT WE REVIEW
- THE COMMUNICATIONS WE ISSUE

THE WORK WE DO

- ANALYTICS
- CORRELATION
- FRAUD DETECTION AND INVESTIGATION
- AUTHORITATIVE GUIDANCE / RESEARCH

THE WORK DONE THAT WE REVIEW

- DID AN AUDITOR DO THE REVIEW OR DID AI EFFECTIVELY DO THE REVIEW?
- HOW DID AI CONTRIBUTE TO SIGNIFICANT JUDGMENTS?
- CAN WE DETERMINE WHETHER THE WORK PERFORMED COMPLIES WITH PROFESSIONAL AND ORGANIZATIONAL GUIDELINES AND POLICIES?

THE COMMUNICATIONS WE ISSUE

- HOW WAS THE AUDIT ISSUE (FINDING) DEVELOPED?
- HOW WAS THE AUDIT REPORT CREATED?
- WHAT APPROVAL PROCESS WAS USED OVER THE AUDIT REPORT?
- HOW WILL FOLLOW-UP BE HANDLED?

OPPORTUNITIES FOR THE FUTURE

- CREATION OR ACQUISITION OF AUDIT EVIDENCE
- ANALYSIS OF ORGANIZATIONAL DATA WITH CROSS-REFERENCES TO PUBLIC/PRIVATE DATA
- LOOKING FOR ORGANIZATION PRIVATE, CONFIDENTIAL, OR SENSITIVE DATA WITHIN AI DATA CONSTRUCTS
- EMPLOYING GENERATIVE AND AGENTIC AI

GENERATIVE AI

GENERATIVE AI REFERS TO ARTIFICIAL INTELLIGENCE SYSTEMS CAPABLE OF CREATING NEW CONTENT—TEXT, IMAGES, MUSIC, CODE, AND MORE—BY LEARNING PATTERNS FROM VAST DATASETS. UNLIKE TRADITIONAL AI, WHICH PRIMARILY ANALYZES OR CLASSIFIES DATA, GENERATIVE AI PRODUCES ORIGINAL OUTPUTS THAT DIDN'T PREVIOUSLY EXIST

AGENTIC AI

AGENTIC AI REFERS TO AI SYSTEMS CAPABLE OF INDEPENDENT DECISION-MAKING AND ACTION, OPERATING WITH MINIMAL HUMAN INTERVENTION TO ACHIEVE SPECIFIC GOALS. UNLIKE TRADITIONAL AI THAT REACTS TO INPUTS, AGENTIC AI PROACTIVELY IDENTIFIES TASKS, DEVELOPS STRATEGIES, AND EXECUTES THEM BASED ON ITS UNDERSTANDING OF THE SITUATION AND OBJECTIVES. THIS CAPABILITY IS ACHIEVED THROUGH MULTI-AGENT SYSTEMS LEVERAGING LARGE LANGUAGE MODELS (LLMS) AND COMPLEX REASONING

POTENTIAL USE OF AI

- AUDIT FOLLOW-UP
- GENERATING CONTROL DOCUMENTATION – RECONCILIATIONS, CONFIRMATIONS AND DOCUMENT REVIEWS
- FULL DATA ANALYSIS
- COMPLIANCE TESTING
- CONTINUOUS AUDITING IN REAL TIME
- RISK AND FRAUD DETECTION
- IT LOG ANALYSIS
- EDR/XDR MONITORING
- COMMUNICATIONS

TOP 5 BUSINESS USES OF AI

- TO CREATE WRITTEN CONTENT – 52%
- TO INCREASE PRODUCTIVITY – 51%
- TO AUTOMATE REPETITIVE TASKS – 40%
- ANALYZING LARGE AMOUNTS OF DATA – 38%
- CUSTOMER SERVICE – 33%
- (ENHANCING CYBERSECURITY IS AT 26%)

- Percentage information from www.isaca.org/ai-pulse-poll

AI DANGERS

- DISCLOSURE OF INFORMATION THAT IS PRIVATE, PERSONAL, OR OTHERWISE PROTECTED (ONLY 41% OF PROFESSIONALS BELIEVE THESE ETHICAL ISSUES ARE BEING PROPERLY ADDRESSED.)
- AI CAN GENERATE FALSE CONCLUSIONS
- LOSS OF CRITICAL AUDIT SKILLS
- CAN BE USED BY BAD ACTORS – HARD TO DETECT

AI DANGERS

- NEED FOR AI SKILLS (89% OF DIGITAL PROFESSIONALS SAY THEY WILL NEED AI TRAINING IN THE NEXT 2 YEARS TO KEEP THEIR CURRENT ROLES.) (45% SAY WITHIN THE NEXT 6 MONTHS)
- NEED FOR A FORMALIZED AI POLICY – NOW ONLY 28% OF ORGANIZATIONS HAVE SUCH

AI ETHICS AND GOVERNANCE

- DATA QUALITY AND SYSTEM TRANSPARENCY
- APPLICABLE REGULATIONS
- ACCOUNTABILITY
- NEED FOR PROFESSIONAL SKEPTICISM
- LOSS OF FUNDAMENTAL AUDIT SKILLS
- HUMAN CRITICAL THINKING AND INVESTIGATION NEEDED

PRIVACY AND CONTROL

- CAN AI SAFEGUARD ORGANIZATION DATA?
  - PUBLIC INSTANCES
  - PRIVATE INSTANCES
- IMPACT OF HACKING / RANSOMWARE / EXFILTRATION
- DO WE NEED TO VERIFY AI RESULTS?
- CAN AI RESULTS BE INDEPENDENTLY VERIFIED?

AI TOOLS AND PRIVACY – J.P. MORGAN

YCNGROUP™

- AI TOOLS GENERATE LETTERS, BUSINESS PLANS, IMAGES AND VIDEOS
- WHEN YOU ENGAGE WITH AI, THESE TOOLS ARE "LEARNING" FROM EVERY INTERACTION WITH YOU
- CHATBOTS CAPTURE AND STORE EVERY QUERY OR PROMPT YOU ENTER, ALONG WITH INFORMATION FROM YOUR PROFILE AND THE DATA GLEANED FROM YOUR COMPUTER EQUIPMENT, SUCH AS YOUR IP ADDRESS

CHATBOTS

- RECORDS AND SAVES EVERY TRANSACTION – EVEN IF DELETED
- CAPTURES USER PROFILE INCLUDING IP ADDRESS, LOCATION, PHONE NUMBER, LOGON DATA, DEVICE INFO (MAKE/MODEL), BROWSER COOKIES, NETWORK ACTIVITY, ETC.
- ALSO GATHERS INFO FROM YOUR SOCIAL MEDIA PAGES.

WHAT ABOUT COPILOT?

According to Microsoft: **First, the Positives**

- MS 365 COPILOT OPERATES MULTITENANT
- DATA IS ENCRYPTED BOTH AT REST AND IN TRANSIT
- COPILOT RESPECTS MS PERMISSION MODELS
- USER PROMPTS, RESPONSES, AND DATA NOT USED FOR TRAINING AI MODELS
- MS 365 COPILOT IS COMPLIANT WITH ENTERPRISE-GRADE PRIVACY AND SECURITY STANDARDS

WHAT ABOUT COPILOT?

According to Microsoft:

- **MS PURVIEW IS A UNIFIED PLATFORM OF SOLUTIONS FOR GOVERNING, PROTECTING, AND MANAGING AN ORGANIZATION'S DATA. IT PROVIDES TOOLS TO HELP ORGANIZATIONS PREVENT COPILOT FROM ACCESSING OR SHARING HIGHLY CONFIDENTIAL CONTENT WITHOUT PERMISSION**

WHAT ABOUT COPILOT?

According to Microsoft:

- **COPILOT ALIGNS WITH ZERO TRUST PRINCIPLES – VERIFYING EVERY USER, DEVICE, AND RESOURCE REQUEST**
- **MS 365 COPILOT INCLUDES PROTECTION AGAINST AI-SPECIFIC THREATS LIKE PROMPT INJECTION ATTACKS**

WHAT ABOUT COPILOT?

According to Microsoft:

- **WHEN COPILOT USES WEB QUERIES VIA BING, USER AND TENANT IDENTIFIERS ARE REMOVED AND THE QUERIES ARE NOT USED FOR TRAINING LLMS OR SHARED WITH ADVERTISERS**
- **ORGANIZATIONS CAN USE PURVIEW TO AUDIT COPILOT INTERACTIONS INCLUDING PROMPTS AND RESPONSES TO DETECT INAPPROPRIATE OR RISKY ACTIVITIES.**

WHAT ABOUT COPILOT?

According to Microsoft:

- **WHEN COPILOT USES WEB QUERIES VIA BING, USER AND TENANT IDENTIFIERS ARE REMOVED AND THE QUERIES ARE NOT USED FOR TRAINING LLMS OR SHARED WITH ADVERTISERS**
- **ORGANIZATIONS CAN USE PURVIEW TO AUDIT COPILOT INTERACTIONS INCLUDING PROMPTS AND RESPONSES TO DETECT INAPPROPRIATE OR RISKY ACTIVITIES.**

WHAT ABOUT COPILOT?

According to Microsoft: **Next, the Risks**

- **IF USER PERMISSIONS ARE TOO BROAD OR MISCONFIGURED, COPILOT COULD ACCESS SENSITIVE DATA LEADING TO DISCLOSURE**
- **WHEN COPILOT USES BING FOR SEARCH, BING PRIVACY TERMS GOVERN (CAN BE DISABLED)**
- **IF USERS REQUEST NO LINKS TO SOURCE FILES, COPILOT MAY NOT GENERATE AUDIT LOGS (NEED TO AUDIT THESE SETTINGS)**

CAN AI LIE?

GENERATIVE AI "CREATES" ANSWERS BASED ON IT'S INTERNAL LEARNING AND PROGRAMMING. THE ANSWERS PRESENTED ARE NOT PRE-ARRANGED. IF THE MODEL AND IT'S TRAINING PROVIDE INFERENCE TO A GIVEN ANSWER AND THERE IS NO DIRECT DATA TO CONFIRM OR REJECT THAT ANSWER, IT MAY BE PRESENTED AS FACT (EVEN IF WRONG).

TOKENS

- A “TOKEN” IS A PHRASE, WORD, OR FRAGMENT (1 CHARACTER OR MORE) TAKEN FROM USER QUERIES AND COMPARED TO DATA IN LARGE LANGUAGE MODELS AND OTHER DATA STORAGE.
- TOKEN RELATIONSHIPS ARE USED TO “CREATE” THE ANSWER TO THE QUERY USING ADVANCED MATHEMATICS

INFORMATION SOURCES

- ISO/IEC 22989,42001, ETC.
- NIST – AI RMF 1.0, ETC. – "ZERO DRAFTS" PILOT PROJECT
- AI STANDARDS HUB – WWW.AISTANDARDSHUB.ORG
- AI WATCH – AI-WATCH.EC.EUROPA.EU
- IEEE STANDARDS ASSN – STANDARDS.IEEE.ORG

MORE INFORMATION SOURCES

- ISACA 2025 EUROPE CONFERENCE 10/15-17 IN LONDON
- GARTNER: EMERGING TECH IMPACT RADAR: GENERATIVE AI
- J. P. MORGAN: AI TOOLS AND YOUR PRIVACY: WHAT YOU NEED TO KNOW
- HTTPS://WWW.JPMORGAN.COM/INSIGHTS/FRAUD/FRAUD-PROTECTION/AI-SCAMS-DEEP-FAKES-IMPERSONATIONS-OH-MY

CONCLUSION

AI TECHNOLOGIES ARE TOOLS, NOT TOTALLY UNLIKE SPREADSHEETS OR WORD PROCESSORS. AI OPERATES WITH DIFFERENT INPUT/OUTPUT INTERFACES AND CAPABILITIES. AI MAKES CONCLUSIONS LOOK EASY, BUT LOOKS CAN BE DECEIVING. AI MAY ENABLE USERS TO APPEAR PROFESSIONAL BUT FAIL TO EXERCISE DUE CARE.

CONCLUSION

WATCH FOR CHANGES. THE AI LANDSCAPE IS RAPIDLY CHANGING, BOTH IN TERMS OF CAPABILITIES AND RISKS. AI SYSTEM PROVIDERS WILL UNDERGO PRESSURES TO ADDRESS SOME, IF NOT ALL, CURRENTLY KNOWN RISKS. STAY WELL READ TO BE PREPARED FOR AN OVERALL AI AUDIT. AND NOW ---

ETHICS – REALLY?

- MIS-USING ANY TOOL IS AN ETHICAL CONUNDRUM – LACK OF PROFESSIONAL JUDGMENT (REMEMBER LOTUS 1-2-3 JOB ESTIMATING)
- PROVIDING INCORRECT INFORMATION TO "AUDIT CLIENTS" WITHOUT SUFFICIENT COMPETENT EVIDENTIAL MATTER IS A BREACH OF INTEGRITY
- RELYING ON OTHERS (HUMANS OR TECHNOLOGY) WITHOUT EMPLOYING CRITICAL THINKING AND PROFESSIONAL SKEPTICISM VIOLATES THE DUTY OF DUE PROFESSIONAL CARE

QUESTIONS?

THE END

- STEPHEN W. MINDER
- STEVE@YCNGROUP.COM
- (217) 520-2092