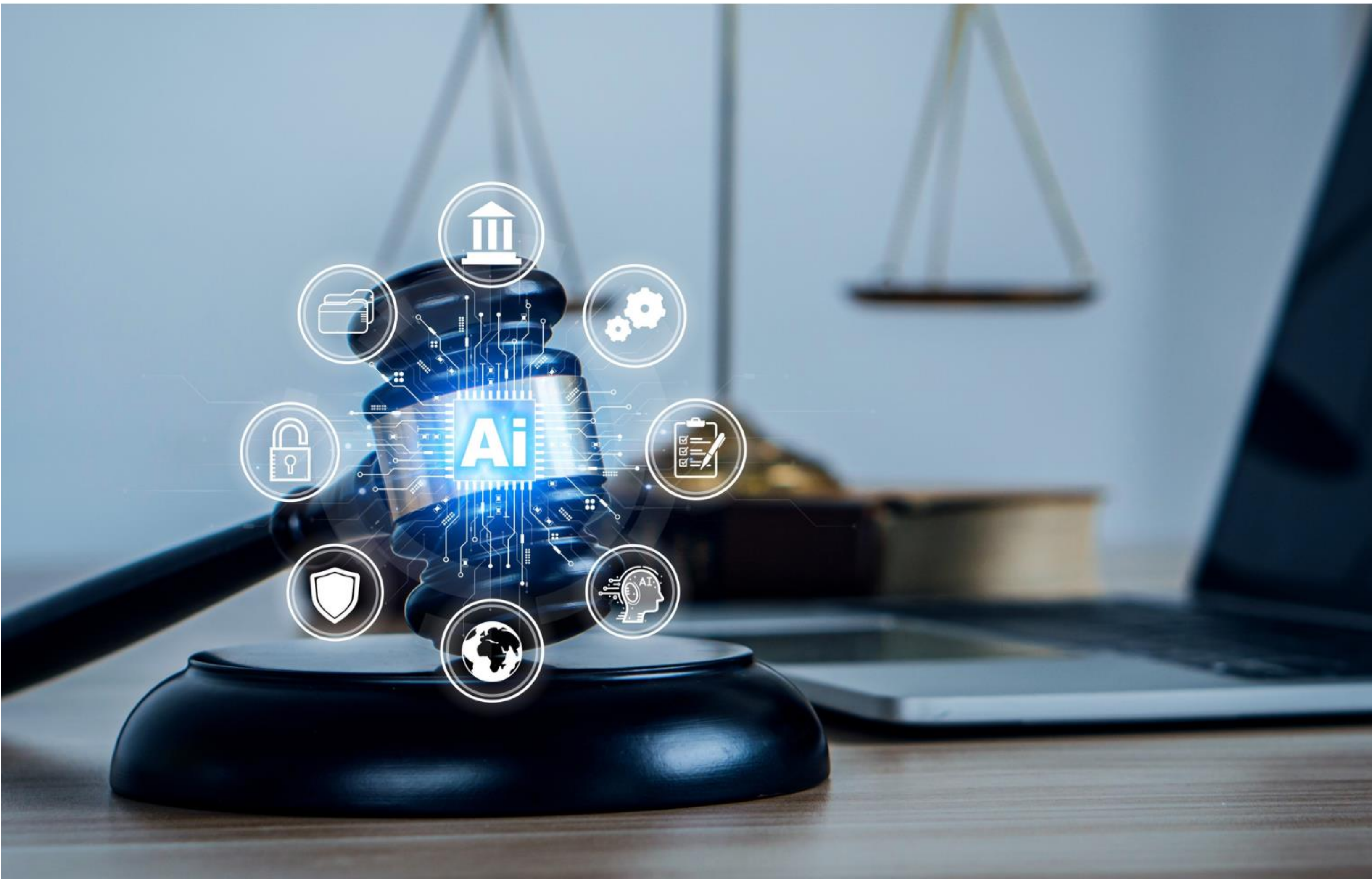
January 2025

INTEGRATING AI: GUIDANCE AND POLICIES FOR PROSECUTORS

Sponsored by:

KARPEL FOUNDATION



Integrating AI: Guidance and Policies for Prosecutors

The National Best Practices Committee and Acknowledgements

The National Best Practices Committee (NBP), convened by Prosecutors' Center for Excellence's (PCE), brings prosecutors together to share ideas, discuss challenges, and develop guidance on today's prosecution best practices.

The NBP includes experienced prosecutors from large and small offices in 30 states. The committee meets on a regular basis to collaborate on creating a vision for the prosecutor's office of the future and issuing papers related to that topic.

The mission of the NBP is to improve the criminal justice system by providing support, guidance, and considerations for prosecutors. The NBP addresses the challenging issues impacting victims, witnesses, the accused, and the community. The guiding principles for NBP's work are a commitment to justice, integrity, ethics, fairness, and equity for all.

See NBP's work on AI and NBP's members at: National Best Practices Committee Webpage.

This paper was written by Antonia Merzon, Senior Attorney at PCE, Jason Kalish, Deputy County Attorney at Maricopa County, AZ, and Bonnie Sard, Senior Attorney at PCE. Marissa D'Amore of PCE created the excellent cover and design.

INTEGRATING AI: GUIDANCE AND POLICIES FOR PROSECUTORS

Executive Summary

Every prosecutor office is facing questions about rapidly emerging generative AI (GAI) technology and how to use it appropriately. This paper addresses the effective integration of GAI in a prosecutor's office. It requires the following steps:

1. Understand GAI's legal and ethical implications for prosecutors

- Review ABA Formal Opinion 512
- Consider state laws regarding collection of sensitive data, data security, and victim protections
- Consider CJIS compliance requirements

2. Assess the office's current use of GAI

- Compile a list of the office's access to (i) GAI tools added to existing programs, (ii) publicly available GAI tools, and (iii) GAI tools developed for lawyers or law enforcement
- Survey or meet with office staff to find out:
  - What GAI tools they are already using
  - How they are using these GAI tools

3. Learn how these current GAI tools work, and the potential impact on confidentiality and security

- Speak with IT staff and/or providers, look at terms of service, and do research to find out:
  - How does an office employee interact with the GAI tools already in use?
  - What happens to the data/information supplied to the GAI tool?
  - What other programs or sources of data does the GAI tool interact with?
  - Can the tool be configured as a "closed" system?
  - How reliable is the output these tools produce?

4. Develop a policy for when and how to use various GAI tools

- Create a policy on acceptable use (or non-use) of various GAI tools

    - See policy template and samples in the appendix and at PCE’s website at: https://pceinc.org/issues/artificial-intelligence/.
- Provide guidance and training to office staff about implementing the policy

5. Assess GAI use by law enforcement agencies and other criminal justice partners

- Determine what tools are being adopted by law enforcement, courts, and other partners
- Assess the ethical and legal implications of this usage on the prosecution of criminal cases
- Assess the admissibility of evidence gathered using various GAI tools

6. Establish a process for evaluating and using new AI technology as it develops

- Designate individuals or create a team to evaluate new tools for prosecutors and criminal justice partners as they evolve
- Update the office’s AI policy and communicate changes to staff

INTEGRATING AI: GUIDANCE AND POLICIES FOR PROSECUTORS

Introduction

Artificial intelligence (AI) is being introduced into the work of prosecutors and law enforcement at an accelerating pace. Prosecutors' Center for Excellence (PCE) is working to assist prosecutor offices as they navigate the influx of AI, particularly generative AI (GAI). This paper provides guidance and information about how prosecutors can begin using GAI technology in a safe and ethical manner. A second paper will discuss how prosecutor offices can begin to harness the power of AI by seeking and developing tools that serve their needs.

PCE may update this discussion periodically to address advancements in AI technology.

Steps for Adopting AI

Every prosecutor office is facing questions about rapidly emerging AI technology and how to use it appropriately. These new tools offer the promise of unprecedented speed, efficiency, analytical power, and creative assistance. If properly utilized by prosecutors, AI technology has the potential to enhance many aspects of their work, such as discovery, victim assistance, evidence analysis, and data collection. AI also has potential deficiencies, including inaccuracy, bias, security weakness, and privacy concerns. Prosecutor offices must be aware of these issues as they begin integrating AI into their practice.

AI based on "machine learning" has been present in criminal justice work for some time. With machine learning, algorithms are designed to detect patterns and predict outcomes. Examples include risk assessment tools used in setting bail and algorithms used for fingerprint and DNA analysis.

Recent advances in generative AI (GAI) are transforming the AI landscape. GAI uses Large Language Models (massive inputs of textual, audio, and visual data) to produce coherent, unique answers in response to human queries using written, graphical, and other formats. These powerful tools raise concerns about responsible usage. ChatGPT is an example of a generative AI program.

With the rapid introduction of GAI products, prosecutor offices, and other criminal justice agencies, must make decisions about whether and how to use them. These are not simple choices in the context of a prosecutor's duties, but rather require a detailed analysis of GAI's potential benefits and risks.

Effective integration of GAI tools involves several steps, including:

1. Understanding GAI's legal and ethical implications for prosecutors
2. Assessing the office's current use of GAI

3. Learning how these current GAI tools and programs work, and the potential impact on security and confidentiality
4. Developing policies for when and how to use various GAI tools and programs
5. Assessing GAI use by law enforcement agencies and other criminal justice partners
6. Establishing a process for evaluating and using new AI technology as it develops

This paper offers considerations and guidance for each step in the process of adopting GAI technology. An AI policy template, as well as samples of AI policies developed by prosecutor offices around the country, can be found in the appendix and on PCE's website at: https://pceinc.org/issues/artificial-intelligence/.

Step 1: Understanding the Ethical and Legal Implications of Generative AI

Ethical Responsibilities

When contemplating the use of any AI tool, prosecutors must consider the legal and ethical implications. Prosecutors (and all lawyers) have ethical duties that have specific application when using technologies. These duties are set forth in the American Bar Association's (ABA) Model Rules of Professional Conduct[1], which have been adopted verbatim or in substance by all state bar associations and legal ethics committees.

In July 2024, the American Bar Association issued Formal Opinion 512 regarding the use of GAI tools.[2] The opinion focuses on GAI's implications for several ethical duties, including the duties of competence, confidentiality, candor, and the proper supervision of attorneys and non-attorneys. Several states have issued similar opinions or guidance on the use of GAI.

The ABA opinion raises important considerations for prosecutors, as follows:

Competence

To act competently in using GAI, lawyers must develop a reasonable understanding of the capabilities, limitations, benefits, and risks of each GAI technology they seek to employ in their practice. Moreover, lawyers cannot inherently rely on the results produced by a GAI tool but rather must independently verify any output it creates. For example:

[1] Model Rules of Professional Conduct, American Bar Association, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents/.

[2] Formal Opinion 512, *Generative Artificial Intelligence Tools*, American Bar Association, Standing Committee on Ethics and Professional Responsibility, July 29, 2024. https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf.

- Before trying out a new GAI feature in a Microsoft Office product, or experimenting with what ChatGPT can do, prosecutors must learn how these tools function and develop a clear understanding of the tool's benefits and its legal and ethical risks.
- When using an AI tool to draft an email, a prosecutor must carefully review the produced text and attachments to ensure the information is accurate, that confidential information is not disclosed, and that the communication is addressed to the correct parties.

Confidentiality

- One of the primary risks associated with a lawyer's use of GAI is the potential for breaching the duty of confidentiality, which requires a lawyer to keep confidential all information relating to a representation. Prosecutors handling criminal litigation must be particularly cognizant of this risk. A prosecutor's duty of confidentiality extends to the facts, evidence, witness information, and other details of a criminal case. The risk that inputting any such information into a GAI tool might inadvertently reveal the information to other users must be carefully evaluated. For example:
    - Before using a GAI tool to draft a case memo, a prosecutor must determine whether inputting the case fact pattern and underlying evidence could reveal confidential information to the tool's developer or other users of the tool.
    - When a GAI tool might be used to analyze phone and text message data obtained with a search warrant, a prosecutor must first determine if inputting this data would divulge confidential information, or if it improperly divulges data that is legally under the control of the issuing court.

Candor

- GAI tools are known to produce false or erroneous results, including inaccurate legal research and analysis. An attorney who uses GAI tools to write briefs or research case law without verifying the results, might end up making a false statement of law or fact to a court. This scenario already has occurred, prompting some courts to require an attorney to affirmatively disclose when AI tools are used in the production of written submissions. For example:
    - Prosecutors using GAI assistance within Lexis or Westlaw must verify that case results are real.
    - Prosecutors using GAI tools to draft legal documents must confirm that case citations stand for the purported holding.

Supervision

- The use of GAI also raises questions about a lawyer's supervisory responsibilities for lawyers and non-lawyers. Clear policies and thorough training are needed for all staff to ensure compliance with ethical and legal duties. Attorneys must ensure third parties and vendors providing law-related data or services to the office are using AI in a manner aligned with lawyers' ethical duties. Supervising attorneys also must take steps to confirm that AI tools do not create confidentiality or security vulnerabilities, and that any contracts with non-lawyer AI vendors conform with the professional obligations of attorneys. For example:

- Supervising prosecutors must provide guidance and training on the appropriate use of ChatGPT and other publicly available GAI tools.
- Prosecutor offices must ensure that vendors providing cloud storage or case management software are employing GAI in a manner that does not risk disclosure of confidential information.

Legal Responsibilities

In addition to ethical duties, prosecutors must comply with legal and regulatory requirements, including federal and state laws and rules related to data security. Any use of GAI must be evaluated against these legal mandates.

Sensitive data and data security

- Laws in most states require prosecutors to safeguard sensitive forms of data that frequently arise in criminal cases, such as personal identifiers, financial account details, and medical treatment information. Some state statutes also mandate government agencies maintain adequate data security protections. Use of AI could potentially violate these provisions if not undertaken conscientiously.

Victim protections

- Many states have victim rights legislation that requires prosecutors to prevent disclosure of a victim's personal identifying information, such as address, date of birth, or social security number. Prosecutors must ensure that AI is not used in a manner that would allow such disclosure.

Criminal Justice Information Services (CJIS) compliance

- Prosecutor offices also must ensure that use of AI complies with CJIS data security directives (to maintain access to NCIC and other CJIS databases). The FBI writes CJIS guidelines but does not accredit programs or services. Even in seemingly secure products, the introduction of a new GAI tool requires a reevaluation of its CJIS compatibility. Does the GAI component download data into another server to process it? Does a GAI program running within a platform retain the file to train itself? Either of these scenarios could present a potential CJIS violation.

Step 2: Assessing Current Office Use of AI

With these ethical and legal considerations in mind, a prosecutor office can start evaluating the appropriate usage of GAI tools and features. This process begins with getting a handle on the GAI tools currently available within the office. These tools generally fall into three categories:

GAI features added to software already in use

- Many commonly used office programs are adding a GAI component. Examples of office software with integrated GAI tools include:
    - Microsoft "Copilot", a GAI-powered chat feature designed to enhance a user's productivity within the Microsoft 365 suite of applications (MS Word, Excel, PowerPoint, etc.).
    - Adobe Acrobat and Reader's GAI Assistant that can summarize and answer questions about the content of PDFs.
    - Zoom's GAI Companion that can record, summarize, and suggest highlights of videoconference meetings, as well as generate related emails and documents.
    - VLex (Lexis) and CoCounsel (Westlaw) are programs that help with research, write questions of witnesses for depositions, and assist in the drafting of memos.

Publicly available GAI tools

- Numerous GAI tools are available to the public online, including ChatGPT. These tools are typically free, chat-based systems in which users can feed the program questions, textual data, audio, graphics, or videos and request analytical or generative output. Examples of publicly available GAI tools include:
    - ChatGPT
    - Google Translate
    - Claude
    - Google Gemini
    - Grammarly
    - DALL-E

GAI tools developed for prosecutors and law enforcement

- GAI tools designed to create specific assistance for lawyers and law enforcement are quickly coming on the market. Some prosecutor offices are exploring the use of these tools. Examples of AI products that could assist criminal litigation include:
    - TrustStat, Truleo, and other programs that use AI to transcribe and analyze body-worn camera recordings.
    - Numerous transcription applications that can create text versions of audio recordings, such as witness statements and jail calls.
    - Textract and Comprehend, two Amazon AI-applications that extract, organize, and analyze text and data from scanned documents.
    - Relativity, and similar programs, that organize and streamline large quantities of digital evidence and case documents for investigative use and discovery.
    - Whisper that transcribes and translates audio recordings such as defendant statements or jail calls.

To find out how their offices are already utilizing GAI, elected and supervising prosecutors might explore the following questions:

- **What tools and programs is the office already using that incorporate GAI?** Create a list of office software and any embedded or associated GAI components. Cataloging the GAI tools currently available within the office may require conversations with IT personnel and office supervisors.
- **Are staff members already using GAI programs?** An office survey can be an effective method for learning how employees are already using GAI, including tools available outside the office network. Office staff may have begun utilizing the GAI components springing up in Microsoft 365 and other pre-existing software. Similarly, staff may have begun exploring, in the office or at home, the use of ChatGPT and other publicly available products in connection with their work.
- **How are staff members using these features and programs?** Surveys and group discussions can also inform the office about what the legal and non-legal staff are doing with GAI tools. What facets of prosecution work are being assisted by GAI? What information are staff members supplying to these applications and programs to get this assistance? What are the positive and negative outcomes of this use?

Step 3: Learning How GAI Tools Work

With a list compiled of the GAI programs and tools being used by office staff, the next area of inquiry centers on understanding how these tools work, and whether utilizing them requires actions that potentially violate rules, laws, or ethical duties.

Questions to ask about the features and processes of each GAI program or tool include:

- **How does a user interact with the GAI tool or program?** Does a user ask it a question and/or supply the program with data (such as with ChatGPT)? Does the program automatically access data and suggest information to the user (such as with GAI features built into word processing programs)?
- **What happens to the data/information supplied to the GAI tool or program?** Does it retain the data or discard it? If it keeps the information, where is it stored? Who has access to it? For how long is it retained? Is the storage system secure? What is the risk of data exposure? For publicly available GAI tools and any tools accessed through a website, a prudent starting point is to assume that all input data is available to the tool's developer. Depending upon the tool, input data may be exposed to other parties as well, including the public.
- **Does the GAI tool or program "learn" from that data?** Would it potentially use office data to answer questions from the public? Or even to other members of the office or law enforcement? What is the risk of data exposure?
- **What other sources of data does the GAI tool or program have?** Is it searching the entire internet for information? Does it rely on data input from specifically defined sources? How might office data be combined with outside data, potentially leading to disclosure?
- **Can the tool or program be configured as a "closed" system?** In other words, can it be set up and used as a self-contained, internal system that keeps any inputs of office data

closed off from the outside world? Or is it always connected to users and data from outside of the office?

- **How reliable is the output these tools and programs produce?** Does the tool or program reliably produce factually and legally correct results? Or is reliability a concern? Does written material meet professional standards?

To answer these questions, an office might consult with its IT services provider and/or internal IT staff. Much of this information is available within a tool's terms of service, or through simple online research. Offices might designate certain staff members with technology interest or experience to investigate the features of GAI applications and programs.

Step 4: Developing Policies for AI Use

Based on what the office learns about each tool and program, it may decide that some uses of GAI features are acceptable, while others are not. For example, asking a GAI program to write a pre-trial motion that requires the input of sensitive case data may violate confidentiality rules and laws, or raise concerns about the professionalism of the office's work product. On the other hand, using it to help write an article in the office's monthly newsletter may not raise legal, ethical, or professional concerns.

Prosecutor offices should strongly consider developing policies and guidance on the use of GAI in connection with prosecution work. Establishing a policy provides direction on the broader questions of when a prosecutor can use GAI in an ethical, legal, and secure manner. A policy also can provide rules and expectations about the use of specific GAI features within the office's existing applications and programs, as well as those generally available online. As the office acquires GAI technology specifically designed for prosecutors, proper use of these tools can be incorporated into the office policy.

Policy and guidance questions to consider include:

- **Which GAI tools and programs are helpful for the office?** What efficiency and analytical benefits do certain features offer? What tasks can they perform? Whose jobs can they support?
- **Which GAI tools and programs produce reliable results?** Are there functions that can be depended upon to produce the level of research, writing, or analysis that a prosecutor office requires?
- **When is it appropriate to supply prosecution data to a GAI program?** Is it acceptable to feed case information into a particular GAI tool (or other sensitive information)? Are there confidentiality issues? Are some tools and programs safer than others? Can they be configured to protect confidential data?
- **What uses of GAI could violate ethical and legal obligations?** How do those considerations translate into the use (or non-use) of specific programs and features?
- **How will the office's GAI policy be communicated to the staff?** Will employees be provided with written copies of the policy? Will they be required to affirmatively agree

to compliance (such as with a signature)? What kind of training on GAI and its approved uses will be needed?

Appendix A contains an AI policy template designed to give prosecutor offices a starting point in considering its individual policy objectives. In addition, several policies developed by prosecutor offices around the country are included as samples in Appendix B. For additional sample policies see PCE's website at https://pceinc.org/issues/artificial-intelligence/.

Step 5: Assessing GAI Use by Law Enforcement

In addition to developing policies about their own office's use of GAI, prosecutors also must consider how GAI tools are employed by law enforcement agencies and other criminal justice partners.

Ethical and legal questions

Law enforcement agencies are rapidly incorporating GAI tools into the policing, investigation, and administrative aspects of their jobs. Prosecutors should know when law enforcement is developing evidence or making arrests based on AI output to properly evaluate the accuracy of these results, as well as the legal and ethical implications of the process. For example:

- Police Reports: Axon has recently developed Draft One to ease the administrative load of writing police reports. The program transcribes audio from police officer's body-worn cameras and then drafts a narrative report based on the transcriptions. Draft One is designed to require officers to edit the first draft before finalizing the report. However, there is no requirement that officers disclose that their report was drafted using AI, and there is no audit trail in Axon to show what portions of a report were AI-generated.[3] At least one prosecutor office has refused to prosecute cases by departments using Draft One based, in part, on ethical concerns about verifying the accuracy of reported information. This is an evolving area where the software or other factors may address these concerns.
- Facial Recognition: Facial recognition software is an AI-powered investigative tool used to identify suspects. Studies have raised concerns that the use of facial recognition software produces disproportionate bias based on skin color.[4] Prosecutor offices should develop a thorough understanding of how any facial recognition software used by local police agencies works and the ethical concerns it might raise, ideally in conversation with these law enforcement partners. With complete information, the office can then determine its position regarding arrests based on facial recognition.

[3] Ng, Alfred, *Did an AI Write Up Your Arrest? Hard to Know*, Politico (September 4, 2024), https://www.politico.com/newsletters/digital-future-daily/2024/09/04/axon-ai-police-reports-00177331.

[4] Turner Lee, Nicol and Chin-Rothmann, Caitlin, *Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color*, Brookings (April 12, 2022), https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/.

Admissibility questions

When AI-enabled programs are being used to develop evidence that proves a suspect's guilt, an important question is whether that evidence will be admissible in court. In other words, will prosecutors be able to present the AI-generated reports, analysis, and exhibits in a manner that satisfy legal evidentiary standards? Federal courts, as well as most states, follow the *Daubert*[5] standard, which assigns the trial judge a gatekeeping role to ensure that scientific evidence is both reliable and relevant. The *Daubert* decision lists five factors that may or may not be helpful in assessing reliability:

1. The theory or technique can be and has been tested,
2. The theory or technique has been subjected to peer review and publication,
3. The theory or technique has a known or potential error rate,
4. The existence of and maintenance of standards controlling its operation, and
5. Whether it has attracted widespread acceptance within a relevant scientific community.

The *Daubert* standard is straightforward when it comes to traditional scientific evidence, such as DNA and fingerprints, where a scientist or technician can explain the collection and analysis processes. When the scientific evidence comes from programs powered by AI, however, the legal determination becomes murkier. Most AI tools are owned by private companies using proprietary technology. These companies often are reluctant or unable to release underlying proprietary information for the purpose of allowing a court to assess the reliability of their products. For example:

- Facial Recognition: Police agencies may purchase facial recognition software that allows them to identify suspects from surveillance footage, with the intention of using a positive identification to make an arrest and submit the case to prosecutors for charging. However, the police would most likely be unable to testify regarding the *Daubert* factors, and the company that created the facial recognition software may not be willing to do so. Given that proof of an AI tool's reliability may not be available, prosecutors may prefer the facial recognition software to be an investigative tool and for police to confirm the identity of the suspect by other means.
- Video Enhancement: Law enforcement agencies might use GAI-powered programs to enhance body-worn camera footage for audio or visual evidence. Without testimony regarding the technological methods employed by the programs, questions may arise about the admissibility of these enhancements.

Similar analysis may be needed for AI tools adopted by other criminal justice partners. Pre-trial agencies may use GAI programs to assess the eligibility of defendants for bail or bond. Courts might employ GAI in evaluating sentencing options. By exploring the potential consequences of

[5] *Daubert v. Merrell Dow Pharmaceuticals, Inc*, 509 US. 579 (1993).

using these technologies at the outset, the prosecutor will be able to express concerns and seek adjustments.

Step 6: Evaluating New AI Technology as It Develops

Generative AI, and other forms of AI, will continue to evolve quickly. Prosecutor offices can prepare for these changes by establishing a procedure for evaluating new AI products and features as they become available. This process also can be applied to new technologies being considered by law enforcement, courts, and other facets of the criminal justice system in their jurisdictions.

Questions to consider in developing an AI review process include:

- **Who will evaluate new AI tools and programs**? Prosecutor offices might consider creating a team or task force of attorneys, support staff, investigators, and IT personnel.
- **What criteria will they be examining**? What are the questions that need to be answered about each new tool or program? Office policies and guidance on the use of GAI could inform the review process.
- **How will the office keep abreast of new AI options**? Are there alerts, research tools, webinars, or other technology information sources that can help the office stay on top of AI changes that are likely to impact prosecution work.
- **How will updates and changes to office policy and guidance on AI be communicated**? As decisions continue to be made about the use of AI features, the office will need an effective, ongoing communication and training approach.

With a proactive approach to AI technology, prosecutors can become leaders in evaluating and adopting advancements in a safe and ethical manner.

Conclusion

Prosecutors are beginning to contemplate the many ways AI might create efficiency, save money, and enhance criminal litigation. AI tools that assist both with individual prosecutions and office management are in various stages of brainstorming and development. Technology companies with existing products for lawyers and law enforcement are racing to create desirable AI tools. At the same time, individual offices are exploring the development of in-house AI tools that serve their specific needs, draw from their data systems, and address prosecutors' confidentiality and security obligations. Our next paper will discuss these advances.

AI has the potential to revolutionize many areas of prosecutors' work. Now is the time to gain knowledge and create policies that allow prosecutors to take advantage of AI's benefits, while maintaining the highest legal and ethical standards. Those offices that do not prepare for AI will be left behind.

APPENDIX A

Prosecutors’ Center for Excellence AI POLICY TEMPLATE

INTRODUCTION

Artificial Intelligence (AI) is a valuable tool that is rapidly becoming integrated into our work. AI has many potential benefits, but it also presents ethical and legal concerns for prosecutors. Before implementing AI tools, we need to consider all of these implications. Of primary concern is that improper use of AI tools can make public otherwise confidential case-related information; can endanger victims, witnesses, and the integrity of our cases; and can expose our lawyers to violations of the ethical rules. This document’s goal is to help ensure our office implements AI tools responsibly.

BACKGROUND ON AI

AI refers to a machine-based system that can make predictions, recommendations, or decisions. AI systems use machine and human-based inputs to perceive environments, abstract such perceptions into models through automated analysis, and use model inference to formulate options.

AI is being integrated into applications and programs used by prosecutors and law enforcement at a rapid rate. AI based on “machine learning” has been present in criminal justice work for some time. With machine learning, algorithms are designed to detect patterns and predict outcomes. Examples include risk assessment tools used in setting bail and algorithms used for fingerprint and DNA analysis. New forms of AI continue to emerge, including generative AI (GAI), which uses Large Language Models (massive inputs of data, including textual, audio, graphic, and video) to produce coherent, unique answers and written material in response to human queries. ChatGPT is an example of a GAI program.

AI AND PROSECUTION: IMPORTANT CONSIDERATIONS

This policy addresses three types of AI tools relevant to our work:

1) AI tools that are currently embedded in existing office-approved programs. AI tools are now embedded into websites and applications that you may use every day. This means that office programs we have been using for years may require us to consider whether and how they can be used in light of newly introduced AI features.

2) Publicly available AI tools. Numerous GAI tools are available to the public online. These tools are typically free, chat-based systems in which users can feed the program questions, textual data, audio, graphics, or videos and request analytical or generative output.

3) AI tools that the office and our criminal justice partners may acquire, including tools being developed specifically for prosecutors and law enforcement. AI tools designed to assist lawyers and law enforcement are quickly coming on the market. Our office, the courts, law enforcement agencies, and other criminal justice partners may now integrate these tools into their work.

4) *[IF APPLICABLE]* In-house AI tools developed by the office. The office is working with its IT staff and service providers to develop AI tools specifically for our use. These tools will rely on internal office data and assist staff with various office needs and tasks.

Each set of AI tools presents its own set of issues and risks. Before you use any AI tools for work-related projects, you must exercise caution and consider what kind of information you are providing the AI tool. This policy relates mainly to GAI tools, but many of the concerns raised about the use of GAI are relevant to other forms of AI. Employees must bear this in mind whenever they are using an application or program in which AI has been integrated. **If you have questions about whether the use of a particular AI tool is problematic, seek help before using it.**

As AI tools and platforms continue to develop, the Office recognizes that these tools and platforms represent innovation that may improve our efficiency, transparency, and our ability to serve the public. However, we also recognize that our duties of competence and confidentiality are paramount and must adhere to the legal and ethical rules that govern our work.

In light of these concerns, we must always be sensitive to several issues in our use of AI, including:

- Confidentiality – We must ensure that the confidential data and materials – such as case and witness details, evidence, and work product – are not improperly disclosed by using an AI tool. Some AI tools may absorb and utilize inputted information to train its AI model, or to answer the questions of future users. This possibility raises serious concerns, as much of the information and data our office gathers, receives, and creates is confidential, and disclosure may be prohibited by statute, ethical provision, or other governing body. **A determination must be made about what data can safely be entered into a specific AI tool before you use it**.

- Human oversight required – AI is an aid to us as a prosecutor office, not a replacement for human judgment, especially in making final decisions about cases. AI tools are not inherently unreliable. They can pick up misinformation and use it to generate convincing but false or erroneous responses, a phenomenon called "hallucination." Because we are ultimately responsible for our work, **employees must review all AI output for accuracy and reliability**.

- Transparency – Our use of AI should be explainable and transparent. We must be prepared to disclose to the court and the defense when AI tools are being used and for what purposes.

- Data Privacy and Security – All sensitive data must be handled securely and in a manner that does not lead to the potential compromise of office data, systems, and networks. Certain types of data – such as personal identifiers, victim information, medical treatment information, and criminal histories – may have specific legal protections. **Extra care must be given when handling sensitive information using AI tools**.

- Supervision and Accountability – Supervisors within the office are responsible for ensuring staff members are using AI tools appropriately and in accordance with office policies. Employees using AI tools improperly will face supervisory action.

- Bias Mitigation – We must take steps to mitigate the risk of bias in our use of AI, which may include periodic audits and validation testing to ensure fairness across demographics.

- Feedback – We must be receptive to feedback from judges, defense attorneys, our law enforcement partners and the community about our use of AI, so that we can improve fairness and ensure public accountability.

OFFICE USE OF AI

Based on the above considerations, this section outlines the acceptable use of AI tools for conducting office work. Attorneys and non-legal staff may use only those AI tools that have been vetted and approved by the Office. Publicly available tools may not provide the necessary security, and information entered into such tools could compromise the confidentiality of our work and our cases.

Attorneys and non-legal staff are NOT PERMITTED to do the following:

- **Use publicly available AI tools for any work-related function**. To the extent that you have downloaded any such tools to your office computer or device, you must delete them. Nor may you use such AI tools on your personal devices for any work-related function.

  Publicly available tools include:

  - ChatGPT
  - Gemini (formerly Bard)
  - Grammarly
  - GoogleTranslate
  - DALL-E
  - DeepAI
  - AlphaCode
  - Q Developer
  - OpenAI
  - *[OFFICES MAY WISH TO ADD OTHER TOOLS TO THIS LIST]*

[IF APPLICABLE, SOME OFFICES MAY WISH TO LIST PERMITTED USES OF PUBLICLY AVAILABLE AI TOOLS AS EXCEPTIONS, SUCH AS:

The following uses of publicly available AI tools are permitted:

- Google Translate or Zoom/Teams for translations that do not involve the input of confidential information (see below definition), such as directions to the office or a request for a meeting.
- Online map applications to search for locations relevant to prosecutions.]
- Translation and transcription services that are produced in a "closed" AI system that does not leak information into the internet.

Consult A Supervisor Before Using Any Online AI Tool To Determine If Its Use Is Permitted.

- **Enter any confidential information into any publicly available software, applications, and chatbots, regardless of whether they use AI**, unless the software, application, or chatbot has been installed by the IT department for that specific purpose. This prohibition includes, but is not limited to, ChatGPT, grammar checkers such as Grammarly, translation assistants such as GoogleTranslate, etc.

  "Confidential information" includes details of an investigation or case, evidence, witness information, criminal history information, and other personal identifying information.[6] It also includes confidential information pertaining to office employees, office policies, and programs. Nor can you endeavor to "anonymize" such confidential data by, for example, changing the names or posing a question using the fact pattern of your case hypothetically.

- **Use any publicly available AI tools to analyze digital evidence**, including but not limited to cellphone, computer, or social media records, or any information obtained via subpoena or search warrant.

- **Rely upon AI in forming legal conclusions or advice,** or rely upon it as a credible source or citation in any court filings or representations to the court or defense counsel. AI may be used to do legal research, as long as the results are verified.

- **Use AI programs to write codes, scripts, or queries** or use programs such as DALL-E to generate photo-realistic images.

[6] For purposes of this policy, "Personal Identifying Information"means a person's name, address, telephone number, driver's license number, social security number, credit card number, bank account number, or any other unique identifier or number that could be used to discover the identity of the person.

- *[IF OFFICE ISSUES DEVICES TO STAFF]* **Download AI tools onto work computers, laptops, or cell phones**. You must delete any AI tools you may already have downloaded on these devices.

- **Use AI programs on personal devices to perform work in a manner inconsistent with this policy**. Employees must follow the office's policies on the use of AI tools when using personal phones, computers, and other devices to conduct office work.

- **Rely upon AI to produce the final version of any letters, reports, policies, or any other document**. All AI output must be reviewed and verified.

Attorneys and non-legal staff are <u>PERMITTED</u> to do the following provided:

- **<u>Your responsibility</u>**. The use of any office-approved AI application or AI program does not negate or undermine your responsibility to make an informed decision about if and how to use the output of an AI application or AI program. For example, if you use an office-approved AI program to summarize the contents of a case file, you must still determine if that summary is accurate and useful for decision-making and comports with the standards of professional conduct required of all employees. You, not the AI program, are responsible for the decisions that flow from an AI-generated work product.
- **<u>Consult a supervisor</u>** before using these tools or if you have any questions about permitted use. *OR* To use these tools, you must attend/view the introductory training module.

Permitted Uses:

- **Use AI features embedded in MS Office, Adobe, and case management programs**. Employees may use AI features embedded in these existing office programs installed on an office device. *[SPECIFY ADDITIONAL PROGRAMS AS NEEDED]*

- **Use videoconferencing platforms with AI features to communicate**. You may also use communication platforms such as *[CHOOSE APPLICABLE]* Zoom and Microsoft Teams to communicate with witnesses, victims, defense attorneys, etc. <u>However, you may not use the translation features on these platforms to conduct witness interviews, nor may you generate transcripts of your conversations on these platforms for any case-related work. Likewise, you should not allow any parties to the meeting to do so</u>.

- **Use VLex in Lexis and CoCounsel in Westlaw to conduct legal research**. <u>However, all research results must be independently verified. Confidential information may not be inputted into VLex or CoCounsel</u>. *[CHOOSE OR ADD APPLICABLE LEGAL RESEARCH PROGRAM]*

- **Use AI tools specifically acquired by the office**. The Office has procured the following AI tools to assist with our work:

    - Whisper (translation tool)
    - *LIST OTHER APPLICABLE TOOLS*

OR

The Office has not yet procured any AI tools. We will continue to update you when we do so and will provide further guidance at that time.

- *[IF APPLICABLE]* **Use AI tools developed internally by the office**. The office has developed certain AI tools specifically for our internal use. You may use these tools for their designated purposes.

- **Evaluate law enforcement use of AI tools**. Local law enforcement agencies *[NAME AGENCY OR AGENCIES]* is currently using an AI tool(s) for the following purpose:

    - Identifying suspects using facial recognition
    - Identifying vehicles using license plate readers
    - Drafting police reports
    - *[NAME OTHER RELEVANT PURPOSES]*

If, in reviewing a case for prosecution, you become aware that law enforcement has used an AI application or AI program as part of the investigation, you must determine that the information produced by the AI application or AI program is accurate. For example, if a law enforcement agency used facial recognition software to identify a suspect, you must review the evidence and determine that there is sufficient information proving the person being charged is indeed the same person that the facial recognition software identified. You may be required to disclose to the defense and to the court that AI was used for these purposes.

[IF APPLICABLE] The office does not accept cases involving the use of the following AI tools:

- *LIST PROHIBITED AI TOOLS HERE*

POLICY UPDATES

Please be aware that our AI policies may change, based on our experience and how new tools evolve. Rapid changes in technology will require us to monitor continuously whether our policies continue to serve us well, and we will need to adjust. We issue this guidance, and the policies outlined above to protect our staff and maintain the confidentiality of information in our possession.

APPENDIX B – Sample Policies

Office of the Special Narcotics Prosecutor, New York

Office of the Special Narcotics Prosecutor

Advisory on Use of Artificial Intelligence

September 3, 2024

Artificial intelligence (AI) is rapidly becoming integrated into our work and embedded into many public websites. Although you may not be aware of it, AI absorbs information you share, and may make it available to other users. It is also in the developmental stages, and information it provides may not be accurate.

Some of you may use AI to help compose letters, emails, and other documents through tools, including but not limited to:

- ChatGPT or Gemini (formerly Bard)
- Microsoft Copilot
- Grammarly
- GoogleTranslate
- DALL-E
- DeepAI
- AlphaCode
- Q Developer
- OpenAI

Before you access AI tools for work related projects, you must exercise caution and be knowledgeable about information you are disclosing. Perhaps of even greater concern, although you may not realize it, **AI tools are now embedded into websites and applications that you may use every day.** While AI has many potential benefits, it also presents ethical and legal concerns.

We are currently developing a detailed policy. This initial guidance is meant to protect our staff from unintentionally sharing confidential information, and to remind staff of the limitations and problematic issues AI presents.

AI refers to a machine-based system that can make predictions, recommendations, or decisions. AI systems use machine and human-based inputs to perceive environments, abstract such perceptions into models through automated analysis, and use model inference to formulate options.

While various forms of AI have been widely used for years, the advent of generative artificial intelligence (Gen AI) — a subset of AI in which machine-based systems create text or images based on predictive models derived from training with large datasets — has elevated interest in and use of AI in legal and other professions.

Be aware that AI has many limitations and flaws. For example, AI can "hallucinate" and generate convincing but false information, and has biases based on the inputs available to AI. As with any emerging technology, there are many unknowns. AI produces a product as requested, but may also absorb and utilize information entered into the tool. Absorbing inputted information allows AI to continue to learn. But it is unclear how this information is stored, and you have no way of knowing how it will be utilized in the future. In other words, ***any information entered in any AI tool may be accessible to the public***. This possibility raises serious concerns for our office, as much of the information and data our office gathers and receives is confidential in nature, and disclosure may be prohibited by statute or agreement without judicial authorization.

As a result of the concerns outlined above, ADAs and non-legal staff are NOT PERMITTED to do the following:

- Enter any confidential information into any chatbots such as ChatGPT, grammar checkers such as Grammarly, transcription assistants such as GoogleTranslate, etc. "Confidential information" includes details of an investigation or case, evidence retrieved from a case, witness information, and other personal identifying information; it also includes confidential information pertaining to SNP employees, office policies, and programs.

- Rely upon AI in forming legal conclusions or advice, or rely upon it as a credible source or citation in any court filings or representations to the court or defense counsel.

- Use AI programs to write codes, scripts, or queries or use programs such as DALL-E to generate photo-realistic images.

- Download AI tools onto work computers, laptops, or cell phones. You must also delete any AI tools you may already have downloaded on these devices.

- Rely upon AI to produce the final version of any letters, reports, or policies.

To the extent that you are following the above guidance prohibiting entry of confidential information and reliance on AI legal research, you are permitted to access websites that utilize AI to assist with certain work-related tasks.

For instance, you may use online map applications to search for locations relevant to prosecutions, Google Translate for initial translations, without allowing it to view unnecessary information, such as phone numbers, and AI tools that assist in the generation of initial drafts of emails and letters that do not contain case specific or confidential information. You must have a reasonable understanding of the capabilities and limitations of the specific AI tool you are using and independently review all AI outputs before use or distribution.

Please be aware that our AI policies may change, based on our experience and how new tools evolve. We issue this guidance and the policies outlined above to protect our staff and maintain the confidentiality of information in our possession. There have been multiple high-profile examples of attorneys sanctioned or cautioned after relying on flawed legal research using Gen AI including:

- **United States v. Cohen, S.D.N.Y., No. 1:18-cr-00602, 12/18/23**

A former attorney for Donald Trump, Michael Cohen, used the chatbot Bard to assist his attorney on legal research for a motion to shorten his probation, leading to the citation in a legal brief submitted to the court of multiple "hallucinated" cases.

- **Mata v. Avianca**

In another case out of SDNY, Mata v. Avianca, the plaintiff's attorneys were sanctioned after submitting a response affirmation citing fake cases. After being ordered to produce full copies of the cases, they could not immediately find them and instead asked ChatGPT for copies. They then submitted these non-existent judicial opinions with fake quotes and citations, all of which had been manufactured by ChatGPT. It is worth noting that, when one attorney began to suspect this might be the case and asked ChatGPT if the cases were real, the chatbot falsely assured him they were real and could be found in Westlaw, LexisNexis, and the Federal Reporter.

The above risks to confidentiality and accuracy are not limited to the legal research:

- **Samsung employees paste confidential source code into ChatGPT**

Samsung banned its employees from using ChatGPT after engineers leaked confidential elements of the company's source code into the chatbot. The company feared that the data may now be revealed to other users, and was uncomfortable with the information being uploaded to servers it cannot access. In the aftermath, other companies also banned ChatGPT.

- **New York City chatbot advises small businesses to break the law**

An AI chatbot set up to help small firms obtain advice on New York legal regulations began telling businesses to break the law. The AI tool "falsely suggested it is legal for an employer to fire a worker who complains about sexual harassment, doesn't disclose a pregnancy, or refuses to cut their dreadlocks".

AI will undoubtedly continue to develop, and may become a reliable, widely used tool in the future. We will continue to monitor its usefulness and reliability, and will issue additional guidance as appropriate.

As we evaluate these new technologies, our top priority remains upholding our legal and ethical obligations. If you have any questions or concerns regarding the use of AI, please contact ADA Ann Heo at ext 919.

Montgomery County District Attorney’s Office, Texas

MONTGOMERY COUNTY, TEXAS

EMPLOYEE POLICY MANUAL

3. EMPLOYEE RESPONSIBILITIES

3.4 Technology Policy

3.4-20b Artificial Intelligence Systems (AI) Use Policy

Purpose

"Artificial intelligence systems" [hereafter referred to as “AI”] *shall mean systems capable of:*
(A) perceiving an environment through data acquisition and processing and interpreting the derived information to take an action or actions or to imitate intelligent behavior given a specific goal; and
(B) learning and adapting behavior by analyzing how the environment is affected by prior actions.
(Sec. 2054.621, Texas Government Code).

“Generative AI” refers to algorithms and models that can generate new content or data, such as images, videos, music, or text, based on patterns learned from existing information.
County recognizes that multiple generative AI platforms are presently available online and appropriate use of generative AI as a tool, individually by an employee and/or in furtherance of a departmental function, may provide significant benefits to employees by enabling them to work more effectively and efficiently. However, the County, as a local government, owns, licenses, or maintains computerized data that includes sensitive personal information, confidential information, or information the disclosure of which is regulated by law (*including as described under Sec. 2054.603, Chapter 2054 - Information Resources, Texas Government Code*) and has certain security related obligations related to such. This policy, therefore, outlines the limitations related to use of generative AI by County employees, so as to minimize security risks to aforementioned data and information, and is intended to further County’s compliance with applicable laws and regulations.

Scope

This policy applies to an employee’s actual or anticipated generative AI platform usage when utilizing any and all County information and/or County information technology resources to access a web/cloud based AI platform, whether directly or through a third party contractor.

Allowable Use:

Subject to the policy on prohibited use stated below, the following are the only allowable uses related to generative AI platforms that are web/cloud based:

1. Generative AI may be used for research and drafting purposes, for example aiding in the generation of new ideas, original content, general forms, formats, documents or prototypes, not otherwise prohibited by County policy or law.
2. Generative AI may be used for artistic or creative purposes, for example in the creation of original content, not otherwise prohibited by County policy or law.
3. Generative AI may be used for training and development purposes, such as creating simulated scenarios and presentations for County authorized employee training and conference engagements.
4. Only generative AI platforms that are pre-approved by the County's Information Technology (IT) Department, whether directly or through a third party contractor, shall be utilized by employees and only for the aforementioned allowable uses.

Prohibited Use:

1. Employees must not utilize generative AI platforms, whether directly or through a third party contractor, that are not approved by the County's Information Technology (IT) Department.
2. Employees shall not directly, or through a third party contractor that utilizes a web/cloud based generative AI platform, upload to an AI platform, enter into an AI platform, and disseminate or expose via an AI platform, any protected, confidential, proprietary, private, copyright protected or other sensitive information and data that is regulated by law, including but not limited to applicable location data, unless said platform is pre-approved by IT. This provision remains applicable whether such data and information is routinely held in County's servers/drives, transmitted to a third party contractor in the ordinary course of business, or otherwise known to an employee through the course of employment and County operations.
3. Employees shall not, in the course of utilizing a generative AI tool, permit or cause an AI or AI platform to access County's secure servers/drives, unless IT has expressly pre-approved such access to the AI platform sought to be utilized.
4. County expressly forbids the use of a generative AI tool in any manner or for any purposes that are illegal, fraudulent or in violation of any County policies.
5. Certain generative AI tools that are available online require acceptance/approval of click-through agreements; employees are prohibited from accepting/approving such click-through agreements without expressly delegated signature authority by County's Information Technology Department or the employee's Elected Official/Department Head.
6. Employees shall not enter any P-Card or credit card/debit card/banking information associated with County and incur, or otherwise allow to be incurred, any charges to the County (directly or indirectly) associated with an AI platform's access or usage, unless such

charges are expressly and previously pre-approved by Commissioners Court and/or Purchasing Department through utilized agreements/POs with designated vendors.

Responsibilities:

Departments and employees anticipating utilization of a generative AI platform by a potential third party contractor of County, are encouraged to seek AI related specifications from the platform or third party contractor, and shall notify IT Department prior to initiating such usage/services. Any resulting security limitations placed by IT on such usage shall be complied with.

Employees are responsible for full compliance with this policy. The IT department may at all times monitor the usage of generative AI on County equipment and resources and investigate and take all appropriate action to address any potential violations of this policy and/or threats to County's networks associated with such.