



AI, HR, Policing, and Bias

Thursday, May 8, 2025

*James Brown, Partner, Liebert Cassidy Whitmore
Neil Okazaki, Senior Deputy City Attorney/Constitutional Policing Advisor, Corona*

DISCLAIMER

This publication is provided for general information only and is not offered or intended as legal advice. Readers should seek the advice of an attorney when confronted with legal issues and attorneys should perform an independent evaluation of the issues raised in these materials. The League of California Cities does not review these materials for content and has no view one way or another on the analysis contained in the materials.

Copyright © 2025, League of California Cities. All rights reserved.

This paper, or parts thereof, may not be reproduced in any form without express written permission from the League of California Cities. For further information, contact the League of California Cities at 1400 K Street, 4th Floor, Sacramento, CA 95814. Telephone: (916) 658-8200.

The Legal Landscape of Artificial Intelligence in Modern Policing

League of California Cities
2025 City Attorneys Spring Conference

James E. “Jeb” Brown

Senior Counsel, Liebert Cassidy Whitmore
Email: jbrown@lcwlegal.com

Neil D. Okazaki

Senior Deputy City Attorney, City of Corona
Email: neil.okazaki@coronaca.gov

1 INTRODUCTION

Artificial intelligence (“AI”) focuses on creating machines capable of performing tasks that typically require human intelligence, such as learning, problem-solving, and decision-making. Ultimately, AI aims to develop machines that can reason, understand natural language, perceive their environment, and act autonomously to achieve defined goals. Introducing AI in policing can enhance efficiency and crime prevention but comes with the need to uphold constitutional rights and prevent discriminatory policies and practices.

Integrating AI into the operational framework of law enforcement agencies represents a transformative shift with the potential to revolutionize crime prevention, resource allocation, and investigative capabilities. Police departments are deploying AI technologies in various capacities, from predictive policing algorithms to target crime hotspots to facial recognition systems to identify suspects. Fueling this rapid adoption has been the allure of enhanced efficiency, data-driven decision-making, and the promise of safer communities.

However, this technological evolution is not without significant legal and ethical challenges. Deploying AI in such a sensitive domain intersects with fundamental constitutional rights. Existing legal frameworks, primarily designed for a pre-digital era, often struggle to adequately address the unique complexities of AI-driven surveillance, data collection, and automated decision-making.

Cities looking to integrate AI into their police department operation should carefully and critically evaluate existing legal frameworks, develop policies, and commit to ethical considerations to mitigate potential risks to civil liberties and ensure this technology is fairly and equitably applied.

2 EXISTING LEGAL FRAMEWORK AND ITS APPLICATION TO AI

Integrating AI into law enforcement practices necessitates carefully examining the existing legal framework to determine its applicability and adequacy in addressing the unique challenges posed by these technologies.

Constitutional Considerations

Fourth Amendment: Protecting Against Unreasonable Searches and Seizures: The Fourth Amendment safeguards individuals from unreasonable searches and seizures. Many AI-driven law enforcement tools significantly implicate this fundamental protection, particularly those involving surveillance and data collection. Several Supreme Court cases provide crucial context for understanding the Fourth Amendment's application in the digital age.

***Carpenter v. United States*, 585 U.S. 296 (2018):** In this landmark case, law enforcement's warrantless acquisition of a person's cell-site location records violated his Fourth Amendment right against unreasonable searches and seizures. The Supreme Court acknowledged that expectations of privacy in the digital age do not fit neatly into existing precedents. Still, tracking an individual's movements and location through extensive cell site records is far more intrusive than the precedents might have anticipated. The Court held narrowly that the government generally will need a warrant to access cell-site location information.

***United States v. Jones*, 565 U.S. 400 (2012):** The Supreme Court held that the police's warrantless placement of a GPS tracking device on a vehicle for an extended period constituted a search under the Fourth Amendment. The Court rejected the argument that there is no reasonable expectation of privacy in a person's movement on public thoroughfares. The unanimous opinion authored by Justice Scalia emphasized that the Fourth Amendment provided some protection for trespass onto personal property. Justice Sotomayor concurred, noting the Government violates a subjective expectation of privacy that society recognizes as reasonable, which is important in an era where physical intrusion is unnecessary to many forms of surveillance. Justice Alito concurred, asserting that the better analysis would be whether the intrusion violated the individual's reasonable expectations of privacy.

***Riley v. California*, 573 U.S. 373 (2014):** The Supreme Court unanimously held that a warrant (absent exigent circumstances) is generally required to search the digital contents of a cell phone seized during an arrest. The Court noted that mobile phones are minicomputers with the ability to store large volumes of pictures, emails, web search history, apps, text messages, and other personal information.

Implications for AI-Driven Surveillance: These cases raise questions about whether AI-driven surveillance technologies, which often involve collecting and analyzing vast amounts of digital data, must adhere to established warrant protocols. The "Time Machine" effect, where AI can analyze historical data to reveal patterns and insights that were previously unknowable, further complicates the Fourth Amendment analysis. Law enforcement agencies must carefully consider whether using AI to analyze large datasets retrospectively constitutes a search and whether a warrant is required for such analysis.

Privacy Considerations: The Center for a New American Security has described the privacy concerns of this emerging technology:

If you just walk down the street in Boston, in New York, in London, you are going to be recorded by many security cameras. Some of them [in] the possession of the local police force, most of them in possession of private companies who just have a security camera. So in society, we have really gotten used to the idea of being photographed constantly. What's new in facial recognition technology is that we're losing the anonymity that used to be associated with being recorded. So it's not just that you walk past a 7-Eleven, and the security camera notes that you're there. There's the possibility that the 7-Eleven will know that you specifically, as an individual, are there, and they know how many times you have passed by in the past few weeks. That's what's really changing in recent years is the ability to analyze this data and correlate it and draw insights from it. It really does raise a whole host of new privacy concerns.

(Peter O'Dowd, *As Facial Recognition Technology Booms, So Do Privacy Concerns* (Dec. 21, 2018) WBUR.)¹

Fourteenth Amendment Equal Protection Considerations: The Fourteenth Amendment guarantees all individuals equal protection under the law, prohibiting discrimination based on protected characteristics. This principle is particularly relevant to the police use of AI due to allegations of potential algorithmic bias.

Brown v. City of Oneonta, New York, 221 F.3d 329 (2d Cir. 2000): The Second Circuit found that police may stop and question members of a minority group without violating the Equal Protection Clause if they are doing so based upon a physical description given by a crime victim. However, the court could find that a racially neutral law or policy has a discriminatory intent and a disparate effect on a minority group.

In the AI context, if algorithms used in predictive policing or facial recognition lead to the disproportionate misidentification of protected classes, cities can expect Equal Protection Clause challenges, even if the algorithm itself was not designed with discriminatory intent.

AI Bias Studies and Mitigation Strategies: The National Institute of Standards and Technology (NIST) published a 2019 report analyzing the performance of 189 facial recognition algorithms. Many of these algorithms were between 10 and 100 times more likely to misidentify a Black or East Asian face than a white face. In some cases, American Indian faces were the most frequently misidentified. (Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use*, WASH. POST, Dec. 19, 2019.)² However, others analyzing this report noted that "NIST found that, 'To the extent there are demographic differentials, they are much smaller,' pointing out error rates in verification-type algorithms are 'absolutely

¹ Found online at <https://www.wbur.org/hereandnow/2018/12/21/facial-recognition-privacy-concerns>.

² Found online at <https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use>.

low,’ generally below 1 percent and many below 0.5 percent.” Jane Parker, *What NIST Data Shows About Facial Recognition and Demographics*, Security Industry Association (2020).³

First Amendment: Preventing Chilling Effects on Free Speech: The First Amendment protects freedom of speech and association. The use of AI for surveillance, particularly of social media activity or protests, raises concerns about potentially chilling lawful expression.

Nat’l Ass’n for Advancement of Colored People v. State of Ala. ex rel. Patterson, 357 U.S. 449 (1958): The Supreme Court recognized the principle of associational privacy, protecting individuals from compelled disclosure of their group membership.

United States v. O’Brien, 391 U.S. 367 (1968): The Supreme Court established a test to determine whether governmental regulation involving symbolic speech was justified. The Court found a government regulation is sufficiently justified if (1) it is within the constitutional power of the Government; (2) it furthers an important or substantial governmental interest; (3) the governmental interest is unrelated to the suppression of free expression; and (4) the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest. (*Id.* at 376-77.)

AI monitoring of public spaces, protest activity, social media, and online platforms must be carefully tailored to avoid infringing on First Amendment rights.

Relevant Legislation

In addition to constitutional principles, several federal and state laws govern the collection, use, and disclosure of electronic information, which are highly relevant to the deployment of AI in law enforcement.

California Consumer Privacy Act (CCPA): On September 24, 2024, the Governor signed a bill that amended the California Consumer Privacy Act (CCPA) to specify that “personal information” includes “artificial intelligence systems that are capable of outputting personal information.” (AB 1008 “Personal Information and AI Systems” effective January 1, 2025, amending Civil Code 1798.140.) By expanding the definition of “personal information,” the bill extended privacy protections to large language models capable of collecting, storing, and disclosing such information.

Artificial Intelligence Training Data Transparency: On September 24, 2024, the Governor also signed AB 2013 which requires AI models to disclose the data used to train the AI model. (AB 2013 “Generative artificial intelligence: training data transparency” effective January 1, 2025, adding Civil Code 3110.)

³ Found online at <https://www.securityindustry.org/wp-content/uploads/2020/02/SIA-NIST-data-and-facial-recognition.pdf>.

Electronic Communications Privacy Act (ECPA): This federal law protects the privacy of electronic communications and sets forth specific requirements for obtaining warrants to access communications content. Police agencies must ensure that the AI system's access to and using this data complies with the ECPA.

For example, if AI intercepts communications protected by the ECPA without consent or a warrant, it could violate the ECPA.

Stored Communications Act (SCA): A part of ECPA, the SCA regulates access to stored electronic communications and transactional records held by third-party service providers. Police typically need a warrant or court order to compel providers to disclose such information.

For example, if an AI system used by police combs through a subject's email account without a search warrant, there would be SCA liability.

3 THE RISE OF AI IN POLICING: APPLICATIONS AND IMPLICATIONS

Integrating AI into law enforcement is driven by the promise of enhanced operational efficiency, improved decision-making capabilities, and a greater capacity for crime prevention. Proponents argue that AI tools can analyze vast datasets with speed and precision exceeding human capabilities, leading to more strategic resource allocation, more informed tactical decisions, and, ultimately, safer communities. However, deploying these emerging technologies also raises significant legal and ethical questions that demand careful consideration.

Examples of Emerging AI Technologies

Predictive policing (e.g., Geolitica): AI-based Predictive policing software uses data and algorithms to forecast criminal activity. By assigning risk scores to specific locations or times, these systems aim to guide police departments in strategically allocating resources like patrols to predicted high-risk areas for crime prevention. The New York Police Department tested predictive policing software as early as 2012. However, concerns exist regarding potential data and algorithm biases impacting fairness and accuracy. Some argue that predictive policing systems could threaten rights protected by the Fourth Amendment, which requires "reasonable suspicion" for detentions. (*See, e.g., Andrew Guthrie Ferguson, Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259 (2012).)

Facial recognition (e.g., Clearview AI): The legal battleground for facial recognition centers on privacy rights, the potential for mass surveillance, and the accuracy and fairness of the technology. This technology enables facial identification of individuals among large crowds and was used to identify many arrested during the January 6 Capitol attacks and the George Floyd protests. *See* FBI, Capitol Violence Images (found online at <https://perma.cc/8ZTC-TVHW>); *See, also*, United States Government Accountability Office, Facial Recognition Technology, GAO-21-518, at 17 (June 2021) (found online at <https://perma.cc/XT39-KV6D>).) However, opponents argue that continuously

scanning and identifying individuals implicates privacy considerations. Furthermore, there is a risk of misidentification. In June of 2024, Robert Williams, who was jailed for 30 hours, settled the first known lawsuit for false arrest resulting from facial recognition technology. (*See Williams v. City of Detroit*, Case No. 21-10827, ECF 73 (June 28, 2024).)

Advanced data analytics (e.g., Palantir Technologies): Police departments increasingly use big data analytics in their daily operations. (Sarah Brayne, *The Criminal Law and Law Enforcement Implications of Big Data*, 14 ANNU. REV. LAW SOC. SCI. 293 (2018)) While powerful for investigations, these tools raise concerns about the scope of data collection, how the data is being analyzed, and who has access to it.

AI drafting of police reports (e.g., Draft One): The use of AI to automate report writing offers potential efficiency gains. Technology exists to enable officers to get a head start on report writing by using AI to draft a report narrative using the officer's body-worn camera audio. The officer then reviews, edits, and signs off on the final report. However, legal questions arise regarding the accuracy and completeness of AI-generated reports, the potential for bias in the AI's language and focus, and the admissibility of such reports as evidence. Ensuring human oversight and accountability for the content of these reports will be crucial.

Integrating these AI technologies into law enforcement presents a complex web of potential benefits and significant legal challenges. As these tools become more sophisticated and widely adopted, police departments should ensure they are used in ways that are consistent with constitutional standards, promote fairness, and maintain public trust.

4 REAL-WORLD EXAMPLES AND THEIR LEGAL CONTEXT

The practical application of AI in policing is no longer a futuristic concept but a present reality, with various law enforcement agencies implementing these technologies. Examining specific examples provides crucial insight into the legal and ethical challenges that arise in real-world scenarios.

LAPD's use of Geolitica to allocate patrol resources efficiently: The Los Angeles Police Department's adoption of Geolitica (formerly PredPol) aimed to optimize the deployment of patrol officers by predicting when and where crimes were most likely to occur. While the intention was to enhance efficiency, this deployment has faced scrutiny regarding its potential to reinforce existing biases in policing. Critics argue that historical crime data, which forms the basis of these predictive models, may already reflect discriminatory policing patterns, leading the AI to target communities of color disproportionately. Some argue this raises Fourteenth Amendment Equal Protection Clause concerns regarding whether the technology leads to a disparate impact on particular racial or ethnic groups, even without explicit discriminatory intent.

FBI leveraging Palantir to disrupt human trafficking networks: The Federal Bureau of Investigation's use of Palantir's advanced data analytics platform to combat human trafficking showcases AI's potential in complex investigations. By analyzing vast amounts of disparate data, including financial records, communication logs, and travel information, Palantir can help identify patterns and connections indicative of trafficking operations. Legal concerns could arise from the scope of the data collection and analysis.

Chicago PD's Strategic Decision Support Centers integrating predictive analytics to reduce shootings: Due to high homicide rates, the Chicago Police Department claims to be the first police department in the nation to use real-time data analysis and predictive software in 2017. By dispatching patrols and social service teams to these areas to engage with at-risk individuals, homicide rates declined by 23% in the first year. (Spandan Kar, *Predictive Policing Examples and Case Studies*, IGNEA (Aug. 5, 2024).⁴ The legal considerations here involve the accuracy and reliability of the predictive models and the potential for them to misidentify individuals or communities as being at high risk.

NYPD's use of ShotSpotter to detect gunfire and improve response times: The New York Police Department's deployment of ShotSpotter, a technology that uses acoustic sensors to detect and locate gunfire, illustrates AI's role in improving response times. While seemingly less controversial than predictive policing or facial recognition, legal questions can arise regarding the accuracy of the technology and its potential for false positives, which could lead to unwarranted police presence in certain areas. A 2024 audit found that "87 percent of the time, ShotSpotter is sending NYPD officers in response to loud noises that don't turn out to be confirmed shootings." (New York City Comptroller Press Release, *NYPD's ShotSpotter Gunshot-Detection System Overwhelmingly Sends Officers to Locations Where No Confirmed Shooting Occurred, New Audit Uncovers*, June 20, 2024 (found online at <https://comptroller.nyc.gov/newsroom/nypds-shotspotter-gunshot-detection-system-overwhelmingly-sends-officers-to-locations-where-no-confirmed-shooting-occurred-new-audit-uncovers>).)

Florida's use of Clearview AI to identify suspects in child exploitation cases: Florida's use of Clearview AI to identify suspects in child exploitation cases highlights the potential of facial recognition technology in combating serious crimes. However, in 2024, Clearview AI settled an Illinois lawsuit alleging its collection of billions of online photographic faces violated the subjects' privacy rights, a deal that attorneys estimate could be worth more than \$50 million. (Kathleen Foody, *Facial recognition startup Clearview AI settles privacy suit*, ASSOCIATED PRESS, June 21, 2024).⁵

⁴ Found online at <https://ignesa.com/insights/predictive-policing-example>.

⁵ Found online at <https://apnews.com/article/clearview-ai-facial-recognition-lawsuit-settlement-5a99ded04630a4e94af01f9f3adf1e29>.

London Police Department's live deployment of real-time facial recognition:

The London Metropolitan Police uses “live facial recognition” as a real-time deployment, comparing live camera feeds against a predetermined watchlist to locate people of interest, such as missing people or those with outstanding warrants. Faces are mapped by software. This dataset is then compared to the watchlist. Where an image is sufficiently similar to someone in its database, an alert is generated and sent to officers who speak to the person of interest. While initially used in small trials and public events like concerts and football matches, it will now be permanently installed for daily use in the summer of 2025 in a South London suburb. (Isiah Thomson, *UK's first permanent facial recognition cameras installed in South London*, The Register, Mar. 27, 2025.)⁶ However, legal challenges have been mounted based on privacy considerations and other UK law theories.

5 GENERATIVE AI: A NEW FRONTIER OF LEGAL CHALLENGES

Generative Artificial Intelligence represents a significant leap in AI capabilities, moving beyond analysis and prediction to creating novel content, including text, images, videos, and even audio. Examples like ChatGPT, DALL-E, and MidJourney have demonstrated the remarkable potential of these technologies. Potential uses for policing -- such as automated report writing, officer training scenarios, and digital forensics -- bring forth a unique set of legal and ethical dilemmas that law enforcement agencies must proactively address.

Potential for Misinformation: One challenge of generative AI is its capacity to create misinformation. The legal ramifications of relying on or disseminating such misinformation could compromise investigations. Police departments must develop protocols to verify the authenticity of any AI-generated information.

Authenticity Concerns (e.g., Admissibility of AI-Generated Evidence): Courtroom admissibility of AI-generated content is largely uncharted territory. Officers relying upon this evidence may lack the technical knowledge to sufficiently validate the foundation for the trustworthiness and admissibility of such evidence.

Ethical Dilemmas in Synthetic Evidence Creation: AI-generated synthetic evidence can be helpful if used ethically with strong safeguards. For example, AI can reconstruct crime scenes visually based on physical evidence, like bullet trajectories, GPS data, and forensics. It can also reconstruct partial data, such as blurry video footage, to better understand events. However, where AI-generated reconstructions are used in investigations or trials, there is a risk of misleading juries or judges, where reconstructions are perceived as “proof” rather than illustrative.

Misuse by Officers: Generative AI is susceptible to misuse, as the technologies could be used for non-legitimate purposes, such as generating false reports, creating misleading social media posts, or creating “deepfakes” for non-legitimate purposes. Departments need to adopt clear policies outlining permissible and prohibited uses and effective oversight mechanisms to mitigate these risks.

⁶ Found online at https://www.theregister.com/2025/03/27/uk_facial_recognition.

Lack of Public Trust: Transparency regarding the use of generative AI will be crucial for maintaining public confidence.

6 POTENTIAL LIABILITY ISSUES

The increasing reliance on AI in law enforcement introduces significant liability risks for both individual officers and the agencies employing these technologies. Errors, biases, or misapplications of AI can lead to wrongful arrests, civil rights violations, and a loss of public trust.

Wrongful Arrests Based on Faulty AI: Inaccurate AI identifications can lead to the detention and arrest of innocent individuals. It has been reported that there have been at least eight confirmed cases of misidentification due to facial recognition technology. (Douglas MacMillan, David Ovalle and Aaron Schaffer, *Arrested by AI: Police ignore standards after facial recognition matches*, WASH. POST, June 13, 2025.)⁷

Discriminatory Policing Practices: If AI algorithms used in predictive policing are found to have a discriminatory impact regarding disproportionate stops, searches, or surveillance of particular communities, individuals may bring Equal Protection Clause claims. Agencies may face *Monell* claims under 42 U.S.C. Section 1983 for failing to mitigate or take corrective action for known biases.

Privacy Violations: The use of AI for mass surveillance, facial recognition, or the analysis of vast amounts of personal data can lead to claims of privacy violations under the Fourth Amendment.

Beyond civil lawsuits, law enforcement agencies can face administrative consequences for the improper use of AI:

Lack of Training and Oversight: Departments are responsible for adequately training their officers on the proper use of AI tools and implementing effective oversight mechanisms to prevent misuse and errors. Departments face accountability for lack of training and oversight.

Failure to Implement Clear Operational Guidelines: The absence of clear and well-defined policies governing the use of AI can create ambiguity and increase the risk of misuse or errors.

Ethical Lapses: Police Departments must establish safeguards to prevent the unethical use of AI.

Thorough training and comprehensive policies are essential for mitigating liability risks associated with AI in policing. Training should cover the technical aspects of AI tools and their limitations, potential biases, and relevant legal considerations. Clear policies should define permissible use cases, establish data handling and analysis protocols, mandate regular audits for bias and accuracy, and outline accountability mechanisms for misuse.

⁷ Found online at <https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/>.

7 ACCOUNTABILITY, OVERSIGHT, AND POLICY DEVELOPMENT

The unique nature of AI requires a thoughtful development of proactive policies.

Department Responsibilities

Police departments are responsible for ensuring the fair and appropriate use of AI technologies. This encompasses several key aspects:

Ethical Responsibility: Police departments must ensure that AI usage aligns with principles of fairness, equity, and respect for civil liberties. Engaging in ongoing ethical discussions and seeking input from community stakeholders are means of deploying AI responsibly to enhance public safety without disproportionately infringing on individual rights.

Maintaining Human Oversight: Critical decisions with legal or constitutional implications must not be solely based on AI outputs but are subject to human review and judgment. Policies should establish clear protocols to define the role of AI in the decision-making process and ensure human accountability for outcomes.

Training: Departments should employ diverse training data to prevent discriminatory outcomes. Topics should include limitations, biases, and proper usage.

Auditing: Departments should implement regular auditing of AI systems to ensure that there are no racial, gender, or socioeconomic biases. Departments should maintain audit logs.

Public Disclosure of AI System Use and Safeguards: Public disclosure can help build trust. Agencies should consider disclosing the types of AI systems used, their intended purposes, capabilities, and limitations, and the safeguards to prevent misuse or errors.

Legal Compliance: Working with the City's legal teams can ensure AI technology aligns with constitutional and statutory mandates.

Developing AI Policies

In the previous decade, some police agencies implemented body-worn camera programs without comprehensive policies governing their use. One legal scholar wrote, “[M]any police departments have adopted body cameras without detailed policies on their use, public access, and data storage. Those body camera policies that do exist can vary considerably.” Elizabeth E. Joh, *Policing Police Robots*, 64 UCLA L. REV. DISCOURSE 516 (2016). Police departments should prepare AI policies to reduce legal risks and build public trust. By clearly defining acceptable uses, establishing safeguards, and outlining accountability mechanisms, agencies can mitigate the potential for constitutional violations, misuse, and erosion of public confidence.

Key Components: An effective AI policy should include several key components:

Clear Definition of AI Use Cases: The policy should explicitly define how AI technologies are authorized for use within the department, outlining the purpose and scope of each application.

Data Governance and Security: Establishing protocols for the collection, storage, use, and retention of data used by AI systems is crucial, ensuring compliance with privacy laws and security best practices.

Transparency: To the extent feasible, police departments should consider releasing information about the algorithms used, their logic, and how they arrive at their outputs.

Human Oversight and Accountability: Clearly defining the role of police officers and supervisors in using AI.

Training Requirements: Mandating comprehensive training for officers and staff on the proper and ethical use of AI tools.

Auditing and Review Processes: Establishing regular audits of AI technologies and updating policies and new technologies and legal standards evolve.

Suggestions for Policy Implementation

Involving Stakeholders: Engaging legal experts, technologists, and community leaders in developing AI policies is advisable.

Develop Use Provisions: Policies should clearly indicate when AI technology is permitted and prohibited.

Routine Reviews: Police departments should regularly review and update policies to reflect advancements in AI technology, changes in legal precedent, and evolving community expectations.

Transparency: Making the AI policy publicly available and communicating clearly about the agency's use of AI can foster trust and accountability.

Lexipol specializes in developing policies for police departments. A 2018 survey showed that 83 percent of California's 200 largest law enforcement agencies used Lexipol policies. (Ingrid V. Eagly and Joanna C. Schwartz, *Lexipol: The Privatization of Police Policymaking*, 96 TEX. L. REV. 891, 958 (2018).) Lexipol has released a policy on generative artificial intelligence use for law enforcement. That policy communicates the benefits and risks of GenAI systems for law enforcement use, designates specific responsibilities to an AI coordinator, outlines the limitations for the use of AI systems and generated content, explains when protected information may be put into AI systems, and outlines the restrictions on the use of AI systems and information.⁸

⁸ Found online at https://www.lexipol.com/wp-content/uploads/2024/05/NEW_Global_National_Generative_Artificial_Intelligence_Use_Policy.pdf.

8 CONCLUSION

AI has enhanced productivity in many fields, including healthcare, education, and scientific research. While the benefits are evident, AI users must thoughtfully consider the legal implications of its use. Police departments are using AI for various purposes, such as identifying suspects, finding stolen vehicles, reconstructing crime scenes, and detecting patterns in criminal activity. The deployment of AI in policing requires balancing enhancing public safety with safeguarding fundamental constitutional rights.