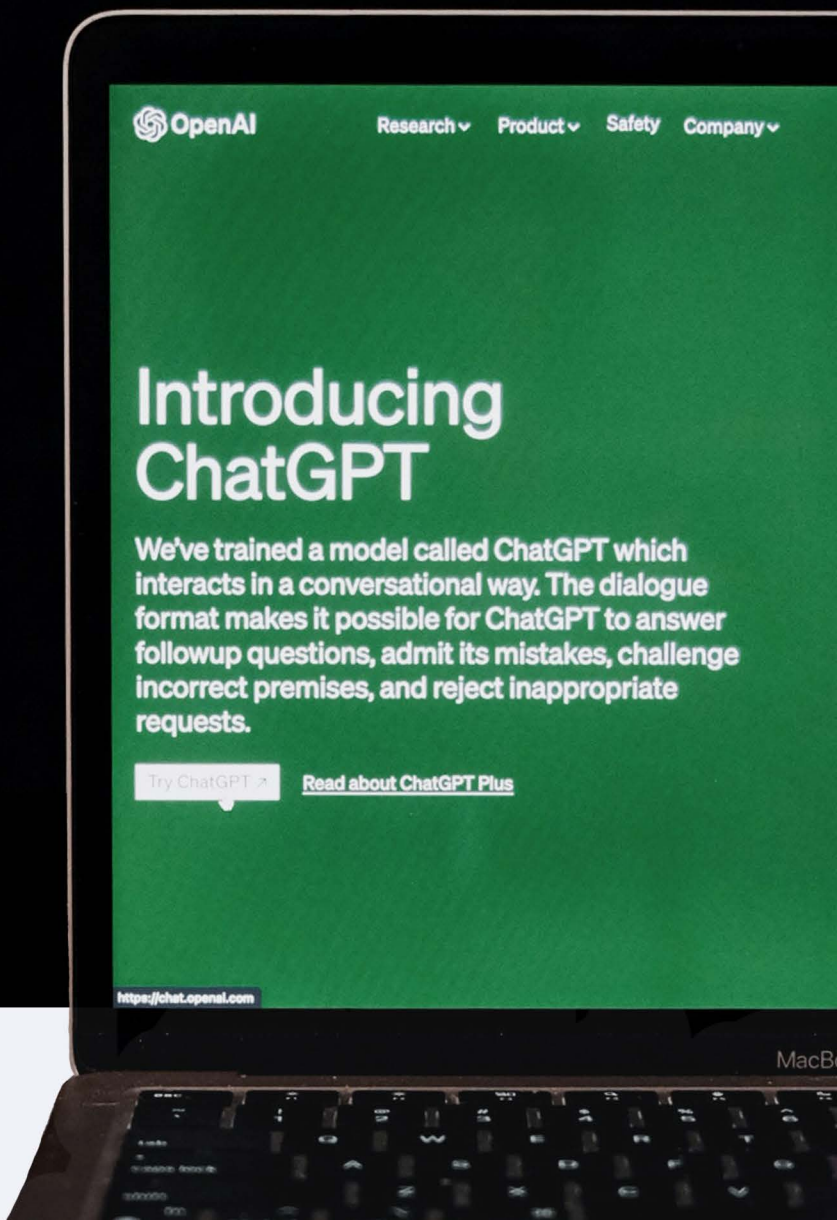
AI Public vs Private Policy Primer

American Consumer Institute

Tirzah Duren & Trey Price

August 2023



ACI
The American Consumer Institute
Center for Citizen Research

Summary

Recent developments in artificial intelligence (AI) have made ongoing regulatory discussions more urgent. With promises of increased productivity and warnings about dangers posed by AI, regulators have been grappling with how to safely reap the benefits of this technology while also mitigating potential harm. The difficult task for regulators is that not all applications pose the same risk. Generally, private sector applications should be integrated into existing legal structures whenever possible. High-risk government applications require more cautious regulation due to the increased risk of harm.

Commercial Applications

AI has already been incorporated into consumer products, with Bing offering AI-assisted[1] search and medical professionals[2] using the technology to aid their diagnosis. These applications show the potential for increased efficiency, but not all outcomes are positive.

Phishing and other scams

One-way bad actors are already taking advantage of AI technology is by using it to create the next generation of phone scams. Through believable voice imitations, scammers can trick a victim into believing that their loved one is in danger with the goal of eliciting ransom payments.[3]

The method is extremely effective. One survey found that of people receiving a voice clone call, 77 percent of recipients reported losing money.[4]

Fortunately for lawmakers, this behavior is already illegal and the Federal Trade Commission (FTC) has warned the public about such phishing scams that imitate a loved one's voice to trick them into sending the scammers money.[5]

IP concerns

To teach generative AI – which refers to algorithms that can create content – the system is trained on massive amounts of data, much of which is copyright protected.[6] This creates tensions between system developers and those who want compensation for the creation of training materials.

Proponents of AI claim that using copyrighted data to train generative AI should be considered fair use as the final product is transformative.[7]

---

[1] Trey Price, "AI Powered Search Engines Could Challenge Google," *American Consumer Institute*, June 5, 2023, https://www.theamericanconsumer.org/2023/06/ai-powered-search-engines-could-challenge-google/.

[2] Trey Price, "AI's Use in Medicine Demonstrates Benefits," *American Consumer Institute*, May 25, 2023, https://www.theamericanconsumer.org/2023/05/ais-use-in-medicine-demonstrates-benefits/.

[3] Amy Bunn, "Artificial Imposters—Cybercriminals Turn to AI Voice Cloning for a New Breed if Scam," *McAfee*, May 15, 2023, https://www.mcafee.com/blogs/privacy-identity-protection/artificial-imposters-cybercriminals-turn-to-ai-voice-cloning-for-a-new-breed-of-scam/.

[4] Ibid.

[5] Alvaro Puig, "Scammers us AI to enhance their family emergency schemes," *Federal Trade Commission*, March 20, 2023, https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes.

[6] John Quinn, "The Clash of Generative AI And Intellectual Property Law: What It Means For Businesses," *Forbes*, May 3, 2023, https://www.forbes.com/sites/forbesbusinesscouncil/2023/05/03/the-clash-of-generative-ai-and-intellectual-property-law-what-it-means-for-businesses/?sh=1eaadc586c01.

[7] Ibid.

The idea of transformative use is common in the music industry.[8] Musicians sample existing work, which is legal so long as it is changed enough to make it sufficiently different from the original. Developers of generative AI argue that the data used in training is changed enough to where the output is not a competitor for the original work and does not constitute copyright infringement.[9]

On the other hand, many artists have gone as far as to say that the outputs AI produces are not originals but amalgamations of its datasets.[10] Some artists are concerned that an AI program using their work would be able to replicate their style and devalue their work in the market.

None of these concerns are unique to AI and are covered by existing legal precedent.

Musician Ed Sheeran recently faced a lawsuit, regarding his sampling of music from artist Marvin Gaye.[11] Ultimately the court determined Sheeran hadn't infringed on copyright, but decisions can go the other way.

The U.S. Supreme Court ruled in March that artist Andy Warhol did infringe on a copyright for one of his renderings of the artist Prince.[12] The decision ultimately hinged on whether the image of Warhol was sufficiently different from the original to not be interchangeable. The court decided that Warhol had infringed as the secondary image and the original were interchangeable and in competition with each other.

The history of court decisions shows that the system is more than capable of handling IP concerns, even with AI. For artistic renderings, the crux comes down to whether the changes are transformative, this should be no different with AI, and is something the current legal system is more than able to handle.

Liability

Like all technology, accidents and negative impacts are bound to occur, AI is no different. However, with the growth of "intelligent" technology some are concerned that there will be no legal framework to punish machines.

One way to make AI regulations as adaptive as possible is to emphasize the need for human control and liability. Luckily, the United States has a substantial legal liability precedent that can be applied to AI.

What this system would look like was explored in the context of radiology by Jonathon Mezrich.[13] In his article, Mezrich discusses how different levels of AI could be incorporate into existing liability law in a medical context. If the AI program is used

[8] Richard Stim, "Fair Use: What Is Transformative?," *Nolo*, https://www.nolo.com/legal-encyclopedia/fair-use-what-transformative.html.

[9] James Vincent, "The scary truth about AI copyright is nobody knows what will happen next," *The Verge*, November 15, 2022, https://www.theverge.com/23444685/generative-ai-copyright-infringement-legal-fair-use-training-data.

[10] Sarah Shaffi, "'It's the opposite of art': why illustrators are furious about AI," *The Guardian*, January 23, 2023, https://www.theguardian.com/artanddesign/2023/jan/23/its-the-opposite-of-art-why-illustrators-are-furious-about-ai.

[11] Ben Sisario, "Ed Sheeran Won His Copyright Trail. Here's What to Know." *The New York Times*, May 4, 2023, https://www.nytimes.com/article/ed-sheeran-marvin-gaye-copyright-trial.html.

[12] Andy Warhol Foundation for the Visual Arts, Inc. v. Goldsmith et al., 598 U.S. 1 (2022). https://www.supremecourt.gov/opinions/22pdf/21-869_87ad.pdf.

[13] Jonathon L. Mezrich, "Is Artificial Intelligence (AI) a Pipe Dream? Why Legal Issues Present Significant Hurdles to AI Autonomy," *American Journal of Roentgenology*, 219:1, February 9, 2022, https://www.ajronline.org/doi/full/10.2214/AJR.21.27224.

as a medical tool with doctors making the final decision, then the doctor would bear liability in case of an error. The principle would be the same as the use of other tools and equipment.

There is even existing legal guidance in cases where AI could become more autonomous. In the context of medical use, if AI is advanced enough to be considered the equivalent of an assistant rather than a tool, then the physician would still be liable through the legal doctrine of vicarious liability. This doctrine establishes liability even in circumstances where multiple people are involved.

If AI were advanced enough to be the equivalent of a doctor, liability still exists. Depending on specific circumstances, the responsibility would fall on the owner of the tool, the manufacturer, or even the professional responsible for its use. In this context the owner would likely be the hospital.

Establishing that a human holds ultimate responsibility for the actions of an AI program will go a long way in encouraging companies and other players to establish safeguards. Additionally, it allows the new technology to fold into the existing legal framework and allows a more flexible approach as AI continues to evolve.

Government Use of AI Poses Additional Risks

Private companies are not the only ones looking to use AI, governments are also incorporating the technology into their functions. While an effective and efficient government is a laudable goal, the authority and power of the institution means there are increased risks if AI is used incorrectly. To manage the risk, government agencies should use increased skepticism to balance benefits with the potential risks to civil rights when implementing this technology.

Surveillance

One of the more dystopian applications is the government use of AI to aid in citizen surveillance. Authoritarian countries such as China offer a case study for the ways AI could undermine democracy and human rights.

Nowhere are the potential dangers of AI clearer than in Xinjiang, where China has been increasingly cracking down on the Muslim Uyghur minority.[14] Through an Integrated Joint Operations Platform, the government uses technologies such as: facial recognition systems, listening to online conversations, and using personal data like health and license information to track and detain individuals.[15]

A report by the Carnegie Endowment for International Peace found that liberal democracies are also major users of AI surveillance technology.[16] Of countries classified as advanced democracies, 51 percent employ AI surveillance compared to 37 percent of closed autocratic states.

Concerns about AI enabling increasingly intrusive surveillance across different government structures have begged the question as to whether AI tools can be created and implemented in a way that complements, rather than undermines, democratic values.

---

[14] Alexander Vindman, Igor Jablokov, Ian J. Lynch, "The World Needs Democratic AI Principles," *The Diplomat*, February 26, 2021, https://thediplomat.com/2021/02/the-world-needs-democratic-ai-principles/.

[15] Steven Feldstein, "The Global Expansion of AI Surveillance," *Carnegie Endowment for International Peace*, September 17, 2019, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

[16] Ibid.

Recognizing the need to protect human rights is an important first step. However, as this technology is adopted it is important for lawmakers to determine what the limits of AI surveillance are to best protect human rights and liberties.

AI surveillance technology is advancing rapidly, and its implementation in government without clear boundaries is a recipe for overreach.

Criminal justice

The use of new technology in the criminal justice and legal system is a double-edged sword. On the one hand, advancements in DNA recognition have helped solve decades-old cases, such as those perpetrated by Joseph DeAngelo, better known as the Golden State Killer. These murders were solved by linking DNA from DeAngelo to that of a relative through the process of forensic genetic genealogy (FGG). This technology has been used to solve over 500 cases so far this year and can also be used to exonerate those who are wrongfully convicted.[17]

Despite the promise of FGG, lawmakers should also appreciate the times when seemingly groundbreaking technologies fell flat when applied to criminal justice. Forensic Bitemark analysis is a prime example that gained popularity after it was used to convict serial killer Ted Bundy.[18]

However, the process, which attempts to match dental imprints to bitemarks left at crime scenes, proved to be flawed.

Currently, Bitemark evidence is subject to increased skepticism due to errors in matching bitemarks to individuals, but this is only after it was used in convictions.[19]

One example is Ray Krone who was convicted with the use of Bitemark analysis.[20] DNA evidence later proved his innocence, but not before he had already served a decade of his life for a crime he didn't commit.

With facial recognition technology already contributing to wrongful arrests[21] and reports highlighting the inaccuracies of the technology across race and gender, the implementation of AI and other technologies into the criminal justice system should be met with more skepticism than other applications.[22]

When the risk is the loss of liberty or even life, then the use of technology should be met with rigorous barriers to entry that prioritize citizens over the government.

---

[17] Michelle Taylor, "How Many Cases Have Been Solved with Forensic Genetic Genealogy?" *Forensic Mag*, March 3, 2023, https://www.forensicmag.com/594940-How-Many-Cases-Have-Been-Solved-with-Forensic-Genetic-Genealogy/.

[18] Caleb Conley, "Ted Bundy: The Bite," *Cumberland University*, https://prod.media.cumberland.edu/wp-content/uploads/2021/07/Ted-Bundy-The-Bite-Coll-Caleb-Conley.pdf.

[19] Michael J. Saks, Thomas Albright, Thomas L. Bohan, et al., "Forensic bitemark identification: weak foundations, exaggerated claims," *J Law Biosci*, 3:3, December, 2016, 538—575, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5570687/.

[20] "Ray Krone," *The Innocence Project*, https://innocenceproject.org/cases/ray-krone/.

[21] Johana Bhuiyan, "First man wrongfully arrested because of facial recognition testifies as California weighs new bill," *The Guardian*, April 27, 2023, https://www.theguardian.com/us-news/2023/apr/27/california-police-facial-recognition-software.

[22] Joy Buolamwini, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *MIT Media Lab*, February 4, 2018, https://www.media.mit.edu/publications/gender-shades-intersectional-accuracy-disparities-in-commercial-gender-classification/.

Issues that apply to both

AI implementation in the public and private spheres has different uses and different potentials for harm. However, there is overlap related to bias and informed consent when interacting with an AI system.

AI bias and discrimination

The issue of decision-making based on imperfect knowledge, lack of data, or internal bias is nothing new. Humans have long struggled with how to overcome these issues and have yet to develop a perfect system. Requiring AI to excel where history has failed is unrealistic.

Instead of AI systems acting as neutral decision makers, analysis of different programs has demonstrated that the biases and decisions that go into the development also pass on human bias and error. Unconscious bias can find its way into the datasets AI uses and affect outputs.

As reported by Reuters in 2018, Amazon ended a program to develop an AI hiring tool after discovering that, due to the high level of males employed by the company, the computer system had learned to discriminate against females.[23] Even after removing gender from consideration, the system still used other information as a proxy for determining gender.

Discrimination in hiring is problematic, but the risks are higher when used in government processes. Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) is a tool used since 2000 and is supposed to accurately predict recidivism risks.

Unfortunately, the system has faced accusations of racial bias – despite not using race as a factor – by overestimating recidivism among African Americans and underestimating among Caucasians.[24] This can happen when the data used to train the model is reflective of racial bias. The program has also been questioned in terms of its efficacy, with untrained professionals who used fewer indicators being able to closely replicate the accuracy of the program.

A report from the National Institute of Standards and Technology notes that bias can enter an AI system in multiple ways including, human bias, systemic bias, and statistical/computational bias.[25] There is no model data set, model person, or model organization that can be used to eliminate errors at each step. Additionally, as noted in a survey of existing research on AI bias, the term "fair" means different things to different people in different places. Therefore, the ability to develop a "fair" or neutral system is impossible.[26]

While there is enough evidence to demonstrate that AI tools fall victim to the same shortcomings

[23] Jeffrey Dastin, "Amazon scraps secret AI recruiting tool that showed bias against women," *Reuters*, October 10, 2018, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

[24] Julia Dressel and Hany Farid, "The accuracy, fairness, and limits of predicting recidivism," *Science Advances,* 4:1, January 17, 2018, https://www.science.org/doi/full/10.1126/sciadv.aao5580.

[25] Reva Schwartz, Apostol Vassilev, Kristen Greene, et al., "Towards a Standard for Identifying and Managing Bias in Artificial Intelligence," *National Institute of Standards and Technology*, March 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.

[26] Eirini Ntoutsi, Pavlos Fafalios, Ujwal Gadiraju, et al., "Bias in data-driven artificial intelligence systems—An introductory survey," *WIREs*, 10:3, February 3, 2020, https://wires.onlinelibrary.wiley.com/doi/full/10.1002/widm.1356.

as those who create them, this doesn't necessarily justify new regulations. Discrimination based on "person's national origin, race, color, religion, disability, sex, and familial status" are already illegal.[27] Clarifying that AI technology is not a shield from legal responsibility will help bring AI into the current legal structure.

While the existing legal structure protects against discrimination, governments should be cautious about rapid adoption given its failed history of eliminating unreliable tools.

Many jobs in the federal government require[28] passing a polygraph test despite doubts by the scientific community that they are reliable.[29] The same rush to implementation by the government can be seen through programs like COMPAS.

Estimates show that over 60 percent of Americans live in jurisdictions that use some type of predictive tool in their legal system.[30] Meaning that while policymakers and academics determine the accuracy of certain models, people are bearing real consequences. Based on this precedent, the government should exercise extreme caution when implementing technology due to the apparent difficulty in reversing those decisions.

AI interactions and disclosure

Wherever possible, increasing consumer awareness can help guide informed consumer decisions. The same is true regarding how consumers choose to interact with AI. A current concern is that as chatbots advance, more businesses and other organizations will incorporate them into customer service systems.

As the American Consumer Institute iterated in its policy paper on data privacy, consumer consent is at the core of how to move forward with many technologies.[31]

Requiring disclosure of AI systems is one relatively low-cost regulation that will empower consumers to determine how they wish to interact with the technology.

---

[27] "Federal Protections Against National Origin Discrimination," *Department of Justice Civil Rights Division*, October 2000, https://www.justice.gov/crt/federal-protections-against-national-origin-discrimination-1#:~:text=Federal%20laws%20prohibit%20discrimination%20based,%2C%20ancestry%2C%20culture%20or%20language.

[28] William Henderson, "How to Prepare for a Security Clearance Polygraph Examination," *Clearance Jobs*, August 25, 2020. https://news.clearancejobs.com/2020/08/25/how-to-prepare-for-a-security-clearance-polygraph-examination/.

[29] "The Truth About Lie Detectors (aka Polygraph Tests)," *American Psychological Association*, August 5, 2004, https://www.apa.org/topics/cognitive-neuroscience/polygraph.

[30] "How Many Jurisdictions Use Each Tool?," *Mapping Pretrial Injustice*, https://pretrialrisk.com/national-landscape/how-many-jurisdictions-use-each-tool/.

[31] Tirzah Duren and Isaac Schick, "Consumer-Focused Data Privacy: A Public Policy Primer," *American Consumer Institute,* April 11, 2023, https://www.theamericanconsumer.org/wp-content/uploads/2023/04/Consumer-Focused-Data-Privacy-Primer.pdf.

Conclusion

AI has the potential for far-reaching impacts, both positive and negative. As lawmakers debate the best way to approach this technology, they should avoid the mistake of painting with too broad a brush.

Private use of AI poses different risks, many of which are already covered by existing law. Incorporating the new technology into current systems avoids regulatory overlap and needless burdens.

While regulations of the private sector should be justified by established harms, government uses should be reined in by the potential for harm and the threat posed to civil liberties. Luckily, constitutionally protected rights can serve as a guardrail for the public use of this technology.

If approached correctly, lawmakers can protect both the efficiencies AI offers and the rights of individuals.