THE GLOBAL LEGAL POST

# UNITED STATES

**David V. Sanker, Ph.D.**
*SankerIP, A Professional Corporation*

This chapter forms part of:

ARTIFICIAL INTELLIGENCE
*Law Over Borders Comparative Guide 2024*

*www.globallegalpost.com/lawoverborders*

## INTRODUCTION

AI is a diverse set of tools that are used by all other industries. Historically, the most widely used AI tool is machine learning. A trained machine learning model can be used, for example, to classify or predict. AI also includes: (i) natural language processing (NLP), which involves recognition of human speech or writing; and (ii) image recognition and processing, such as facial recognition. More recently, generative AI tools can create novel text or images based on human prompts.

Although AI has very broad social and political issues, the analysis here focuses on some of the legal issues surrounding AI, including intellectual property protection, laws intended to limit undesirable use of AI, and guidelines for the use of generative AI.

## 1. CONSTITUTIONAL LAW AND FUNDAMENTAL HUMAN RIGHTS

Because the United States Constitution is written in general terms, many of the constitutional provisions are readily applied in an AI context. The Constitution is also the basis for any fundamental human rights.

### 1.1 Domestic constitutional provisions

The Fourth Amendment and the Fourteenth Amendment of the United States Constitution apply if an AI system affects the rights of people.

The Fourth Amendment limits search-and-seizure, and requires "probable cause, supported by Oath or affirmation." Although an AI system itself may not be able to provide an "oath or affirmation" for probable cause, a user of an AI system can provide it. For example, in Blue Springs, Missouri, AI-enhanced camera technology led to the arrest of a murder suspect in April 2024. See KCTV via Gray Media Group, Inc., (*www.kptv.com/2024/04/28/ai-enhanced-camera-technology-leads-murder-suspects-arrest/*), April 28, 2024. Before the arrest, the police were able to use the AI data to prepare a four-page probable cause statement, with the appropriate "oath or affirmation" provided by a police officer. As long as the data provided by AI is reviewed by a person, there is unlikely to be a Fourth Amendment violation.

The "Due Process" clause of the Fourteenth Amendment prohibits deprivation of "life, liberty, or property" without due process. In particular, it is unlikely that a court would accept a conclusion of an AI system without other support.

However, due process concerns have not prevented violations from occurring. For example, the Unemployment Insurance Agency for the state of Michigan used an AI system (known as MiDAS) to automatically "detect" alleged fraud, and wrongly billed people for unemployment payments plus 400% interest. See Stephanie Wykstra, "Government's Use of Algorithm Serves Up False Fraud Charges," UNDARK (*undark.org*), June 1, 2020. Although the wrongful bills in this example have largely been settled through class action lawsuits, this example shows that the Fourteenth Amendment is not self-executing. People and organizations should consider potential constitutional violations **before** implementing any new programs that use AI without appropriate human oversight.

### 1.2 Human rights decisions and conventions

Courts in the United States uphold the Constitution, statutory laws, and previous binding opinions of higher courts. Because the United States Constitution (and the Bill of Rights, codified as the first ten amendments to the Constitution) is written in broad terms, any party seeking to invoke "human rights" should cite to appropriate provisions in the Constitution and decisions by the Supreme Court on those provisions.

## 2. INTELLECTUAL PROPERTY

AI affects intellectual property rights in several ways:

- use of generative AI tools may lead to loss of intellectual property rights;
- use of generative AI tools may create output that is accused of infringing the rights of authors whose works were used to train the AI tools;
- when an invention uses AI, it can be challenging to (i) identify the inventive features; and (ii) draft patent claims that are not considered an "abstract idea"; and
- when an invention or original work is created by AI, or with the assistance of AI, there are limits on what can be protected.

Some uses of public AI systems risk loss or limit of IP rights. When using a tool like ChatGPT, Claude, Meta Llama, Microsoft Bing, or other generative AI systems, it can appear to the user to be a private conversation. In the absence of a specific contract provision with the generative AI provider, any information supplied to a generative AI tool should be treated as a public disclosure. This forfeits any trade secret protection for that information, forfeits any potential patent rights anywhere outside the United States, and begins a one-year grace period for patent filing in the United States.

### 2.1 Patents

**Inventions that use AI**

The tools and techniques of AI, such as neural networks and convolution kernels, are well-known. Therefore, patentable novelty typically involves other aspects, such as constructing novel inputs for an AI model, modifying the AI training in a substantial way, utilizing AI output in a creative way, or building AI hardware. For example, merely inserting AI into a process that was previously done without AI would not satisfy patentability, even if the process with AI is faster or better. On the other hand, if the inserted AI has been created specifically for a certain use case, it is likely to be patentable.

As an example of creating novel inputs for a machine learning model, some inventions modify raw data to create synthetic data elements. Typically, synthetic data elements apply mathematical operations to groups of raw data items. The set of possible raw data elements to use may be quite small, but there is virtually unlimited flexibility for creating synthetic data elements.

Identifying the key features for patentability is important for patent drafting because it focuses the work of patent attorneys. Under section 112 of U.S. patent law, a patent disclosure must "enable" the invention. And under section 101 of U.S. patent law, the claims of a patent must recite sufficient detail to be more than an

"abstract idea." Good patent drafting generally identifies the patentable elements first, and then supports those elements with claim language and disclosure to satisfy sections 101 and 112.

**Avoid divided infringement**

Applying AI typically occurs in two distinct phases. In the first phase, one or more developers train an AI model and test the model until it produces good results. In the second phase, the model is deployed (e.g., as part of a device or software application) and end users use the deployed model. A single patent claim that requires both training and using an AI model has a problem with divided infringement because there is rarely a single party that performs both the training and the usage.

One solution to the divided infringement problem for AI is to draft two distinct claim sets. A first claim set requires only training the AI model. A second claim set requires only using the trained AI model. The two claim sets (typically in two distinct patents) cover a wide variety of possible infringers.

**Inventions created with the assistance of an AI system**

Inventions created solely by an AI system are not patentable in the United States. See *Thaler v. Vidal*, 43 F.4th 1207 (Fed. Cir. 2022). The more common case is where an AI system contributes to an invention, but one or more humans also contribute to the invention. The United States Patent and Trademark Office (USPTO) addressed this scenario in its February 13, 2024 guidance. Because AI inventors cannot be listed in a U.S. patent application, the USPTO focuses instead on the contributions of people. The guidance is available at *www.federalregister.gov/documents/2024/02/13/2024-02623/inventorship-guidance-for-ai-assisted-inventions*. The guidance helps determine which humans (if any) made contributions to an invention that are sufficient to be designated as inventors. The primary case is *Pannu v. Iolab*, 155 F.3d 1344 (Fed. Cir. 1998). Although the guidance from *Pannu* is somewhat thin, the USPTO also provided two examples on its AI-related resources webpage. There should be more guidance on what constitutes a "significant" contribution over the next few years.

The key point is that companies should create development processes that have at least one **substantial** human inventor. Even if a fully autonomous AI development system could be faster and/or cheaper, it may not be useful if the created inventions cannot be patented.

### 2.2 Copyright

**AI authors**

U.S. copyright law provides no protection for AI-generated content. In particular, if an AI system generates an entire work, there is no copyright protection at all. When an AI system generates portions of a work, the overall work and the portions not generated by AI can be protected by copyright, but the AI-generated portions are not protectable. In "Zarya of the Dawn," the human author wrote the text and used an AI system to generate most of the images. According to a decision by the U.S. Copyright Office on February 21, 2023, the AI-generated images were not protectable.

For AI-generated content, a person generally provides input in the form of a "prompt." A key question for copyright is whether human creativity in the creation of the prompt has an effect on whether the output can be copyrighted. In some cases a person creates a final prompt after many iterations to create a desired effect.

The U.S. Copyright Office currently does not consider the construction of the prompt to add to the creativity of the work, even when there are many iterations and many changes to the prompt by the user. The Copyright Office policy to disregard any creativity in the input prompt was demonstrated in "Théâtre D'opéra Spatial," which is artwork that won an art contest at a Colorado fair. According to the human artist, it took over 600 iterations to get the prompt so that the generated output satisfied his objective. Despite the extensive human input to create the image, the U.S. Copyright Office reasoned that the final image was generated based on a single final prompt, so copyright protection was denied.

To overcome this limit on copyrights for AI-generated work, some authors modify the output **after** it is generated. There is not extensive data on this yet, but sufficient human creativity after AI generation should enable copyright protection.

**Protection of AI with copyrights**

Many AI tools and utilities that use AI are implemented in software, so the source code can be protected under copyright law. However, copyright protection is limited, because it generally only protects against theft by people who have direct access to the source code.

### 2.3 Trade secrets and confidentiality

**Protection of AI-related inventions**

Patents are subject to examination and many patent laws, and this is even more burdensome for AI-related inventions. Because trade secrets are not subject to these requirements, they provide an attractive alternative to patents. In particular, trade secrets:

- do not require a human inventor;
- do not require proof of novelty;
- do not require proof of subject matter eligibility (i.e., no consideration of whether an AI invention is an "abstract idea"); and
- are not subject to the wide variation of patent examiners.

But not all inventions can be kept secret. In many cases, deployment of an invention is inherently visible and thus subject to reverse engineering. In these cases, patent protection is a better option.

**Protection of AI-related data**

In the context of AI, there are almost always at least two datasets to protect as trade secrets. First, the training data for the AI system should be protected. In fact, the training data may be the most valuable asset for many AI use cases. In particular, it can take a considerable investment of time and money to collect and classify the training data. And the training data can be supplemented in the future to build even better training sets.

Second, a trained AI model can be protected as a trade secret. A trained AI model can be considered as a large batch of parameters (e.g., neural network weights), and these parameters are not visible when the model is used.

### 2.4 Notable cases

Because of the widespread use of AI, there has been extensive legislative and judicial activity. Most of this activity is still in progress, but there have been at least three significant developments. First, President Biden issued an Executive Order on AI on October 30, 2023, which addresses many facets of AI. Second, the USPTO issued inventorship guidance on February 13, 2024 to specifically address the situation where AI systems are acting in an inventive capacity. Third, the U.S. Copyright Office issued rulings regarding copyrights for works that include AI-generated content. The USPTO inventorship guidance is discussed above in Section 2.1 and the Copyright Office rulings regarding AI-generated content is discussed above in Section 2.2.

President Biden's Executive Order on AI is an extensive list of issues related to the use of AI and recommendations on how to safeguard that usage. The Executive Order is more comprehensive than the EU AI Act in Europe, but the Executive Order is less detailed. There are two key takeaways from the Executive Order.

First, the value of the Executive Order will depend on how it is implemented by government agencies and Congress. Even the best guidance will fail if there is not substantial additional work to turn the Executive Order into meaningful oversight.

Second, it is unclear whether the Executive Order will have much impact on intentionally bad actors. For those that want to exploit AI in socially harmful ways, governments will need more than an Executive Order or laws. Good actors need to develop AI systems to identify and counteract the malicious usage of AI.

For the full text of the Executive Order, go to *www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence*.

## 3. DATA

There are many facets to the use of data by AI systems. As discussed in Section 2.3 above, training data and AI model data can be protected as trade secrets. If the AI training data includes personal data, the collection or usage of that data may violate privacy laws. And the usage of copyrighted material for training an AI system may be a copyright violation.

### 3.1 Domestic data law treatment

**Data privacy**

Although not specifically directed toward AI, the United States has both federal and state laws to protect personal data.

Federal laws include:

- the Health Insurance Portability and Accountability Act (HIPAA), which limits sharing of sensitive patient data;

- the Fair Credit Reporting Act (FCRA), which limits usage of data collected by consumer reporting agencies; and
- the Children's Online Privacy Protection Rule (COPPA), which prohibits collection or use of personal information from and about young children.

Many states have enacted further laws to restrict collection or use of personal data by AI.

**Use of copyrighted works for AI training**

Many developers of AI systems use copyrighted works to train their models. In general, training an AI system uses millions or billions of training inputs, and the training can ingest huge volumes of copyrighted content. It is an open question whether training and using an AI model constitutes copyright infringement. One high-profile lawsuit was filed by the New York Times against Microsoft and OpenAI on December 27, 2023 in a federal court in New York (Case 1:23-cv-11195). Because the training of an AI model does not directly produce output, infringement contentions usually focus on using a trained model.

An important consideration is whether using a trained model is "fair use." Section 107 of the U.S. Copyright Act defines "fair use" as a legal doctrine that "promotes freedom of expression by permitting the unlicensed use of copyright-protected works" in certain circumstances. There are four primary factors for fair use analysis, two of which are:

- the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- the effect of the use upon the potential market for or value of the copyrighted work.

Because of the tenuous connection between the training inputs and any specific generated output, both of the factors above support the fair use argument. In particular, any generated output uses very little from any one specific input, and the generated output is unlikely to have any effect on the market for any of the training inputs. However, if a specific output is close enough to a specific input that was used for training, the fair use argument is weaker.

### 3.2 General Data Protection Regulation

Many companies need to transfer data between Europe and the United States. The European Commission issued an "adequacy decision" on July 17, 2023 for the new Europe–U.S. Data Privacy Framework (DPF). This new framework is voluntary and provides specific ways to transfer personal data consistent with European law. Companies can join the DPF by certifying compliance with the Department of Commerce. See *www.dataprivacyframework.gov*.

### 3.3 Open data and data sharing

The United States launched the National Artificial Intelligence Research Resource (NAIRR) pilot program on January 24, 2024. See *new.nsf.gov/focus-areas/artificial-intelligence/nairr*.

NAIRR points out that "AI holds the potential to accelerate discovery and innovation and help solve critical societal and global challenges. However,

many researchers lack the necessary access to the computing, data, software and educational resources needed to fully conduct their research and to train the next generation of researchers." Therefore, "NAIRR aims to bridge this gap and ensure that AI resources and tools are accessible to the broad research and education communities in a manner that advances trustworthy AI and protects privacy, civil rights and civil liberties."

In an era where many people are concerned that Big Tech has a growing monopoly of AI, NAIRR is taking an open, sharing approach to make sure that data and tools are available to everyone.

### 3.4 Biometric data: voice data and facial recognition data

Currently the United States does not have laws to specifically address voice and facial recognition data. The National Academies of Sciences, Engineering, and Medicine says that there is an urgent need for such federal laws. See *www.nationalacademies.org/news/2024/01/advances-in-facial-recognition-technology-have-outpaced-laws-regulations-new-report-recommends-federal-government-take-action-on-privacy-equity-and-civil-liberties-concerns*.

In the absence of federal law, many states have enacted their own laws, for example:

- The Illinois Biometric Information Privacy Act (BIPA) requires entities that collect biometric data to maintain a written policy about the collection and storage of biometric data and to obtain informed consent from individuals subject to biometric data collection.
- Under the Capture or Use of Biometric Identifier (CUBI) Act in Texas, a private entity may not capture a person's biometric identifier for a commercial purpose unless the entity informs the person prior to capturing the biometric identifier and receives the person's consent to the collection.
- The California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) specify that biometric data, including voice data and facial recognition data, is protected information.
- The Virginia Consumer Data Protection Act (VCDPA) requires controllers to obtain consent before processing a consumer's biometric data.

## 4. BIAS AND DISCRIMINATION

Large datasets can reveal hidden insights, but they can also hide biases that lead to a disparate impact on protected groups.

### 4.1 Domestic anti-discrimination and equality legislation treatment

The United States has many laws that address discrimination, including the Equal Credit Opportunity Act, Title VII of the Civil Rights Act of 1964, the Fair Credit Reporting Act, The Federal Trade Commission Act, the Americans with Disabilities Act, the Age Discrimination in Employment Act, the Fair Housing Act, and the Genetic Information Non-discrimination Act. All of these laws apply when using AI.

In January 2016, the Federal Trade Commission (FTC) released its Big Data Report. In the report, the FTC stated that "To maximize the benefits and limit

the harms of big data, the Commission encourages companies to consider the following questions raised by research in this area." The four questions are:

- How representative is your dataset? Companies should consider whether their datasets are missing information about certain populations, and take steps to address issues of underrepresentation and overrepresentation.
- Does your data model account for biases? Companies should consider whether biases are being incorporated at both the collection and analytics stages of big data's life cycle, and develop strategies to overcome them.
- How accurate are your predictions based on big data? Companies should remember that while big data is very good at detecting correlations, it does not explain which correlations are meaningful.
- Does your reliance on big data raise ethical or fairness concerns? Companies should assess the factors that go into an analytics model and balance the predictive value of the model with fairness considerations.

When the FTC evaluates an AI algorithm for possible illegal discrimination, it looks at whether the model includes ethnically based inputs, or proxies for such inputs. The FTC also reviews the outcomes regardless of the inputs, to determine whether a model appears to have a disparate impact on people in a protected class. When there is disparate impact, the FTC reviews the company's justification for using that model and considers whether a less discriminatory alternative could achieve the same results.

## 5. CYBERSECURITY AND RESILIENCE

AI and cybersecurity are separate topics, but they are frequently discussed together. AI can be used by bad actors to steal data or compromise systems (e.g., ransomware), but AI can also be used by good actors to bolster cybersecurity protection.

### 5.1 Domestic technology infrastructure requirements

The National Institute of Standards and Technology (NIST) implements a wide range of regulations that apply to federal agencies and organizations or contractors that work with the federal government. NIST has developed two frameworks to deal specifically with cybersecurity. The first framework is NIST SP 800-53, which is mandatory for all federal agencies. The second framework is NIST SP 800-171, which applies to government contractors in order to protect Controlled Unclassified Information (CUI). The second framework 800-171 applies, for example, to universities that are supported by federal grants, manufacturers who supply products to federal agencies, and companies that provide services to federal agencies.

The two security frameworks are also different in their scope. Whereas the 800-53 framework entails comprehensive security for all federal systems and requires regular formal assessments, the 800-171 framework is focused on protecting CUI in non-federal systems with compliance by self-assessment and documentation.

Even for companies that do not fall under the mandatory requirements of 800-171, voluntary compliance can be valuable to establish credibility in the market and can enable a company to obtain government contracting opportunities in the future.

## FREQUENTLY ASKED QUESTIONS (FAQS)

**What guidance can you give for using generative AI?**

**Potential loss of confidential information when using generative AI**

See above, Section 2, introduction. Entering confidential data as a prompt to a generative AI tool can lead to loss of rights for the data entered.

**Potential infringement by using output from generative AI**

See above, Section 3.1. There are ongoing lawsuits by content creators whose works have been used to train AI models. Although the current lawsuits are against the companies that created the models, lawsuits could be filed against users of generative AI as well.

**Potential inability to secure IP protection when using generative AI**

See above, Sections 2.1 and 2.3 regarding AI inventors and AI authors. Although IP protection is not available for inventions or works created entirely by AI, patent protection is available when there is at least one human inventor with a significant contribution to the conception of the invention, and copyright protection is available for portions of works not created by AI. When considering copyright protection, it is also possible for a person to modify the output created by an AI system, and the modifications may be enough to enable copyright protection.

**For an invention that uses AI, how can I decide whether to seek a patent or keep it as a trade secret?**

See Section 2.3 above. First, decide what aspects of a new invention are actually inventive (which are generally not the AI). Then determine whether those inventive aspects can be kept secret (e.g., not subject to easy reverse engineering).

**Can I actually get a patent for a software system that uses AI?**

After the 2014 U.S. Supreme Court decision in *Alice v. CLS Bank*, 573 U.S. 208 (2014), "subject matter eligibility" under section 101 of U.S. Patent Law has been a hot issue. In addition, there has been a wide range of opinions about section 101 among patent examiners, appeal board members, and courts. During enactment of the current U.S. Patent Laws in 1952, relevant testimony stated that patentable subject matter may include "anything under the sun that is made by man." But now, some examiners consider it a very high hurdle just to be eligible for patent protection, and routinely reject patent claims for allegedly being directed to an abstract idea.

It is definitely still possible to get software patents (e.g., software that uses AI), but it is more work to prepare a patent application and good patent claims, and success/quality will depend on the assigned examiner and the selected patent practitioner.

## 6. TRADE, ANTI-TRUST AND COMPETITION

### 6.1 AI-related anti-competitive behaviour

**Competition concerns for generative AI**

The Federal Trade Commission (FTC) recognizes that generative AI is rapidly "becoming a basic part of daily life." See "Generative AI Raises Competition Concerns," FTC Technology Blog, June 29, 2023, available at *www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns*. This is a concern because of an imbalance in who has access to training data, computational resources, and human talent. The cost of computational resources is particularly

relevant when creating a base model for generative AI costs millions of dollars (e.g., it cost over USD 100 million to build OpenAI's GPT-4 model). Some form of government intervention may occur in the future.

**AI pricing collusion**

Historically, pricing collusion involves agreements between people to fix prices so that they are not competing against each other. The U.S. government can address this type of pricing collusion under either section 1 of the Sherman Act or section 5 of the Federal Trade Commission (FTC) Act.

But research now shows that algorithmic pricing by AI systems can "consistently learn to charge supra-competitive prices, without communication with one another." See "Artificial Intelligence, Algorithmic Pricing, and Collusion" by Emilio Calvano *et al*., American Economic Review, Vol. 100, No. 10, October 2020, pp. 3267–97. The question now is whether such algorithmic pricing could be construed as illegal under current laws. If not, the question is whether lawmakers could find the result sufficiently undesirable that they draft new laws to address it.

### 6.2 Domestic regulation

In the U.S., antitrust law is a collection of mostly federal statutes. These include the Sherman Act of 1890, the Clayton Act of 1914, and the Federal Trade Commission (FTC) Act of 1914.

## 7. DOMESTIC LEGISLATIVE DEVELOPMENTS

### 7.1 Proposed and/or enacted AI legislation

Most AI legislation is enacted by individual states, with considerable variation in goals. In 2023, at least 25 states proposed AI legislation, and many were enacted. For example, California proposed 11 AI laws, one of which has already been enacted. One theme is that states want to inventory their current use of AI. For a substantially complete review of the pending and enacted AI legislation, see the National Conference of State Legislatures at *www.ncsl.org/technology-and-communication/artificial-intelligence-2023-legislation* and *www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation*.

### 7.2 Proposed and/or implemented government strategy

The Executive Order by President Biden on October 30, 2023 laid out an extensive strategy for AI: see Section 2.4 above. The Executive Order created a roadmap for many other federal agencies, including:

- USPTO (see above, Section 2.1, for February 13, 2024 inventorship guidance);
- USPTO (April 29, 2024: Request for Comments Regarding the Impact of the Proliferation of Artificial Intelligence on Prior Art, the Knowledge of a Person Having Ordinary Skill in the Art, and Determinations of Patentability Made in View of the Foregoing);
- NAIRR (see Section 3.3, above, for January 24, 2024 pilot program to make sure AI data and AI tools are widely available);
- NIST (see *www.nist.gov/artificial-intelligence*, describing the work of NIST to achieve the directives in the Executive Order); and
- FTC (see January 25, 2024 compulsory production orders regarding AI to Alphabet, Inc., Amazon.com, Inc., Anthropic PBC, Microsoft Corp., and OpenAI, Inc.).

## AUTHOR BIOGRAPHY

**David V. Sanker, Ph.D.**

After nearly 20 years as a patent attorney at Morgan Lewis, David launched his own boutique patent firm SankerIP in February 2024. SankerIP provides a full range of services for IP portfolios, including patent prosecution, IP strategy, due diligence, and freedom-to-operate analysis. David frequently writes and speaks on AI topics, and was recognized as a Top AI Attorney in California by the Daily Journal in 2019 and 2024. As a patent attorney, David has worked with a wide variety of technologies, including software, AI, semiconductor devices, cybersecurity, medical devices, data visualization, and database architecture. Prior to law school, David worked as an assistant professor of mathematics for three years and as a software engineer and database architect for 12 years. David earned both his Ph.D. (mathematics) and J.D. from U.C. Berkeley. His education and 15 years of experience in teaching and software development enable him to better understand new inventions and work with both inventors and patent examiners.