Managing the Legal Risks of AI on Intellectual Property and Confidential Information

Written By Kristie Prinz, Esq.

Abstract

This article addresses the AI legal risks encountered by consulting psychologists and managers leading organizations in the United States pertaining to intellectual property and confidentiality. The article first provides an overview of the relevant legal principles of patent, copyright, trademark, trade secret and confidential information. The article then discusses three significant risks: the risk that AI use will result in infringement of third-party intellectual property; the risk that an organization or individual will be unable to protect ownership rights in an invention or work developed using AI; and the risk that the use of AI will result in the loss of confidential information and/or trade secrets. Finally, the article discusses specific guidance to consultants and managers on steps they can take to manage the legal risks.

Keywords: artificial intelligence, AI, intellectual property, IP, confidential information, legal risks

Implications for Consulting Psychology

With the increasing prevalence and use of artificial intelligence (“AI”), it is inevitable that consulting psychologists and organizations will utilize generative AI tools. However, the use of AI carries certain legal risks to IP and confidential information. This article explains these legal risks and discusses the steps that can be taken to manage those risks.

Managing the Legal Risks of AI on Intellectual Property and Confidential Information

As artificial intelligence ("AI") tools are more widely adopted and utilized by business organizations to perform everyday tasks and operations, organizational and consulting psychologists and managers leading organizations are increasingly facing new legal risks pertaining to AI, not only with respect to how they manage the use of AI in their own businesses but also with regard to how they advise their clients as AI issues arise which have legal implications.

Although consulting psychologists and managers leading organizations will potentially be required to anticipate and manage numerous risks arising from AI, including both legal as well as business-focused risks, the scope of this article is limited to addressing the management of AI legal risks pertaining to intellectual property ("IP") and confidentiality in the United States. In addition, this article will provide specific guidance to consultants and managers on steps they can take to manage those legal risks.

Overview of Legal Principles

To understand the AI legal risks pertaining to IP and confidentiality, consultants and managers need to first understand the legal principles that apply to both concepts. "Intellectual property" has been defined by the United States Patent and Trademark Office (the "USPTO") to constitute "creative works or ideas embodied in a form that can be shared or can enable others to recreate, emulate or manufacture them" (USPTO, 2024). The four forms of protection available to IP are patent, copyright, trademark and trade secret, each of which are further discussed below, along with examples of each concept.

Patent

In the United States patents are granted by the USPTO. The owner of a U.S. patent obtains a monopoly over the invention described in the patent, which monopoly enables that owner to exclude third parties from making, using, offering for sale, or selling the invention in the United States and its territories and possessions, or alternatively, from importing the invention into the United States and its territories and possessions (USPTO, 2024). There are three types of patents: (1) utility patents, which protect inventions on a new or useful process, machine, article of manufacture, or composition of matter (e.g. the patents protecting the inventions comprised by a smartphone are utility patents); (2) design patents, which protect a new, original, ornamental design for an article of manufacture (e.g. the patents protecting a uniquely shaped beverage bottle or the unique form of a classic car are design patents); and (3) plant patents, which protect inventing or discovering and asexually reproducing any distinct and new variety of plant (e.g. the patents protecting a unique variety of a rose or a fruit tree plant are plant patents). In the case of utility and plant patents, a U.S. patent generally grants a protection period of 20 years from the date the first non-provisional application for a patent was filed (35 U.S.C. §154 (2024)). In the case of a design patent, the protection period is 15 years (35 U.S.C. §173 (2024)).

Copyright

In the United States, copyright is automatically granted to an author of an “original work of authorship” from the time the work is created in a fixed form (Copyright Office, 2024). An example of a copyright protecting an original work of authorship is a copyright protecting the original manuscript of a novel or journal article. Copyright can also protect original code in a software program, or an original video recording of a training program. Notwithstanding the foregoing, copyright does not protect original ideas, except to the extent those ideas are incorporated into an original work of authorship, in which case the work but not the ideas are protected.

A U.S. copyright grants certain exclusive rights to the author, including: (1) the right to reproduce the copyrighted work; (2) the right to prepare derivative works based on the copyrighted work; (3) the right to distribute copies of the copyrighted work to the public; (4) the right to display the work publicly; (5) the right to perform the work publicly and (6) the right to authorize others to exercise all of the foregoing rights (17 U.S.C. §106 (2022)). The general rule regarding copyright is that it lasts for the life of the author plus an additional 70 years (17 U.S.C. §302(a) (2022)). For anonymous and pseudonymous works and works for hire, the general rule is that copyright lasts for 95 years from first publication or 120 years from creation (17 U.S.C. §302(c) (2022)).

While copyright in the United States automatically exists from the moment it is created in a tangible form of expression, registration with the U.S. Copyright Office ("Copyright Office") is required to be eligible to enforce the owner's exclusive rights in the U.S. court system (17 U.S.C. §411(a) (2002)). In addition to the benefit of being able to enforce exclusive rights in a court of law, registration provides the following benefits in the United States: (1) it provides a record of ownership in the searchable Copyright Office database of ownership; (2) it establishes prima facie evidence of validity and the facts stated in the certificate if granted before or within five years of publication; (3) it makes the owner eligible for statutory damages, attorneys' fees, and costs when made prior to infringement or within three months after publication of the copyrighted work; and (4) it permits the owner to establish a record with the U.S. Customs and Border Protection ("USCBP") for protection against the importation of infringing copies (17 U.S.C. §§408-412 (2002)).

Trademark

A trademark is any word, phrase, design, or a combination of the foregoing which identifies a good or service which is used in commerce. An example of a well-known trademark is the scripted "Coca Cola" logo that is used in connection with the goods described as "beverages and syrups for the manufacture of such beverages." Certain limited, local trademark rights exist under common law to use of a trademark in a limited geographic scope from the moment a trademark is first used by an owner in connection with a good or service.

In the United States, a trademark owner may protect its rights in a trademark through registration, which is available at both the state and federal levels. The USPTO grants federal trademark registrations, which convey to owners the following benefits: (1) a record of ownership in the USPTO's publicly searchable database; (2) the legal presumption of owning the trademark and having the right to use it; (3) the basis for trademark protection in other countries; (4) the right to bring a lawsuit to enforce the trademark in federal court; (5) the right to publicly use the federal trademark registration symbol in order to put the public on notice of the registration; and (6) the right to record the registration with USCBP, in order to stop the importation of goods with an infringing trademark (USPTO, 2024). In contrast to patents and copyrights, trademarks can last forever for as long as the owner continues to use the mark in interstate commerce for the specified use; however, federal trademark registrations have to be renewed with subsequent maintenance filings on a periodic basis in order to maintain the registered rights (USPTO, 2024).

Trade Secret

A trade secret is any non-public, proprietary item of business information that gives the owner a competitive advantage over a third party. An example of a trade secret is the proprietary Coca Cola formula, which is a distinctive beverage formula. To qualify as a trade secret, an item of proprietary information must meet 3 requirements: (1) it must have actual or potential, independent economic value because it is not generally known; (2) it must have value to third parties who cannot legitimately obtain it; and (3) it must be subject to reasonable efforts to remain secret (USPTO, 2024). Unlike patents, there are no required procedural formalities to maintain proprietary information as a trade secret. However, proprietary information ceases to be a trade secret once any of these 3 requirements are no longer met (USPTO, 2024).

The significance of maintaining the status of a trade secret notwithstanding the lack of procedural formalities is that, in the event that the trade secret is ever misappropriated, the trade secret owner will then have a potential legal claim in a court of law for trade secret misappropriation, which will only be available to the extent that the trade secret owner can meet the burden of proof required to establish that a trade secret actually existed.

Confidential Information

Confidential information is a non-public, proprietary item of business information, which may include mere ideas and may or may not rise to the level of a trade secret. As in the case of trade secret, there are no required procedural formalities for confidential information protection: protection is also dependent on secrecy. Also, as in the case of trade secret, the information must have been known only to a limited group of persons and the rightful owner must have made reasonable efforts to maintain its secrecy. Notwithstanding the foregoing, the primary distinction between the two concepts is that unlike with trade secrets, confidential information is not required to have separate commercial value.

Legal Risks Arising from the Use of AI

Having an understanding of these basic concepts is critical to understanding the three most significant legal risks arising from AI use, which organizational consultants and managers increasingly encounter, not only in advising their clients but also in managing their own businesses: (1) the risk that AI use will result in infringement of third-party intellectual property; (2) the risk that an organization or individual will be unable to protect ownership rights in an invention or work developed using AI; and (3) the risk that the use of AI will result in the loss of confidential information and/or trade secrets.

The Risk that AI Use will Result in Infringement of Third-Party IP

One of the most significant risks that organizational consultants and managers will encounter as a result of AI use is the risk that, by using AI, an organization or individual will inadvertently create works that infringe third-party IP resulting in potential legal claims and liability.

This concern arises from the fact that many of the new AI-based software tools available for use by businesses and individuals are generative platforms that train from data consisting of huge archives of images and text, which the software uses to determine patterns and relationships, to create rules, and to then make decisions and predictions in response to a prompt (Appel et al., 2023). While it is not inherently the case that a generative platform training on archives of images and text will create a heightened risk of copyright infringement or plagiarism for platform users, the possibility exists that one or more images and texts that the AI has trained on may be copyrighted and that a particular generative prompt may create content, which is derivative of one or more of these copyrighted texts or images, and is then used all or in part to form a new or derivative work by the platform user without the authorization of the copyright owner. Any such use of generative content could potentially be deemed to constitute copyright infringement, since only a copyright owner has the right under U.S. Copyright Law to authorize the creation of a derivative work from a copyrighted work. Alternatively, in the event that the generative content is a trademark or service mark, and the infringing use constitutes a confusingly similar use in connection with another good or service, such use could potentially be deemed to constitute trademark infringement. Furthermore, even if a particular use of generative content by a platform user does not rise to the level of intellectual property infringement, the use of generative content may still inadvertently constitute plagiarism of an original author's content, if the use of generative content uses ideas, thoughts, or content by an original author without appropriate attribution or credit (Caldwell, 2023).

Lawsuits have already been filed in U.S. courts alleging infringement of intellectual property as a result of generative AI, so the legitimacy of this generative AI concern has already been somewhat substantiated. For example, Thomson Reuters, the parent company of Reuters News, has filed a lawsuit in a Delaware federal court accusing Ross Intelligence of illegally copying headnotes from Thomson Reuters' Westlaw legal research platform to train an AI-based search engine (Brittain, 2024). Getty Images has filed a lawsuit in the UK against Stability AI alleging that Stability AI"s AI-image generator Dream Studio had copied millions of its images (Brittain, 2023). Stability AI was also named as a defendant, along with Midjourney and DefiantArt, in a class action suit filed in a San Francisco federal court filed by a group of visual artists alleging that the software infringed on the artists' copyrighted works to create images in those artists' styles without permission (Brittain, 2023).

Litigation arising from AI generative tools is anticipated to focus on whether the use of copyrighted works is protected by the fair use doctrine. The fair use doctrine is an exception to copyright law principles codified in Section 107 of the Copyright Act of 1976, allowing copyrighted works to be used without the copyright owner's authorization, based on an evaluation of four factors: (1) the purpose and character of the use, including whether the use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work; and (4) the effect of the use upon the potential market for the value of the copyrighted work. (17 U.S.C. §107 (2022); Appel, et al., 2023; Moreno, 2023; Wiggers, 2023). It is anticipated that, as in past litigation testing the application of the doctrine of fair use to other fact patterns dealing with new uses of technology, that the decisions may rest on whether the courts view a particular use of a generative AI tool to be "transformative" (e.g. whether it adds new expression, meaning or message to an original work) as opposed to “competing in the same market as a substitute for the work of the original creator” (Appel, et. al., 2023; Moreno, 2023).

The Risk that an Organization or Individual will be Unable to Protect Ownership Rights in an Invention or Work Developed Using AI

A second significant risk that organizational consultants and managers will encounter as a result of AI use is the risk that an organization or individual will be unable to protect ownership rights in an invention or work developed with the use of AI. Inventions or work arising all or in part from outputs of user instructions to a generative AI prompt will not in all cases be protectable, since the availability of patent or copyright protections will be dependent on the degree of human involvement and contribution in the development of the invention or work. An organization or individual seeking to protect ownership rights in an invention or work developed with the use of AI will have to be able to demonstrate to the appropriate federal agency that the human contributions in developing the IP were sufficient to meet the standards required in order to receive the protection sought under the applicable U.S. patent or copyright law.

The USPTO and Copyright Office have already received filings seeking protection of IP developed with the use of AI, and have each issued guidance to practitioners and the public on how filings with their offices pertaining to IP developed using AI will be handled.

Earlier this year, the USPTO announced its *Inventorship Guidance for AI-Assisted Inventions* in the Federal Register, effective February 13, 2024, providing “instructions to examiners and stakeholders on how to determine whether the human contribution to an innovation is significant enough to qualify for a patent when artificial intelligence (AI) also contributed” (Vidal, 2024). In this Guidance, the USPTO reiterated its position, affirmed by the Federal Circuit in the 2022 decision in *Thaler v. Vidal,* that “an inventor must be a natural person, and by extension, any joint inventor must be a natural person”, but stated that “the use of an AI system by a natural person(s) does not preclude a natural person(s) from qualifying as an inventor (or joint inventors) if the natural person significantly contributed to the claimed invention" (89 Fed. Reg. 30, 10045 (2024)).

Building on the existing inventorship framework and "significant contribution" test defined in the Federal Circuit's 1998 decision in *Pannu v. Iolab Corp.*, the USPTO then defined the principles that would be applied in determining who qualified as an inventor where generative AI was involved with the development: (1) how the person constructed an AI prompt with respect to a particular problem "to elicit a particular solution from the AI system"; (2) whether the person took "the output of an AI system and [made] a significant contribution to the output to create an invention" or "[conducted] a successful experiment using the AI system's output"; (3) whether the person "[developed] an essential building block from which the claimed invention derived" in the "designing, building, or training of the AI system" (e.g. "the natural person(s) who design(s), build(s), or train(s) an AI system in view of a specific problem to elicit a particular solution could be an inventor, where the designing, building, or training of the AI system is a significant contribution to the invention created with the AI system"); and (4) whether the person was merely "owning or overseeing an AI system in the creation of an invention, without providing a significant contribution to the conception of the invention" (89 Fed. Reg. 30, 10048 (2024)).

The USPTO clarified that its guidance is intended to apply to "not only utility patents and patent applications but also to design and plant patents and patent applications" (89 Fed. Reg. 30, 10049 (2024)). It also specifically warned that anyone involved with submitting a patent application involving an AI-assisted invention has a duty to disclose any evidence that a "named inventor did not significantly contribute to the invention because the person's purported contribution(s) was made by an AI system", as well as a duty to inquire "whether and how AI is being used in the invention creation process" (89 Fed. Reg. 30, 10049-10050 (2024)).

The Copyright Office announced the publication of its own AI guidance in August, 2023, which separately defined how works containing material generated from AI would be evaluated by the agency (88 Fed. Reg. 51, 16190-16194 (2023)). In its guidance, the Copyright Office stated that the test to be employed on a case-by-case basis would focus on whether the AI contributions by a particular AI tool resulted from “mechanical reproduction,” meaning “mechanical processes or random selection without any contribution by a human author,” or an author’s “own original mental conception to which [the author] gave visible form” (88 Fed. Reg. 51, 16192-16193 (2023)).

If a particular work containing AI-generated content is deemed to “contain sufficient human authorship to support a copyright claim,” then the Copyright Office would grant copyright registration on the aspects of the work that were authored by a human (88 Fed. Reg. 51, 16192-16193 (2023)). On the other hand, if the “traditional elements of authorship” comprised by such work were “produced by a machine,” then the Copyright Office would refuse registration of the work on the determination that it “lacks human authorship” (88 Fed. Reg. 51, 16192-16193 (2023)). The Copyright Office emphasized that the key determinations in its evaluation would focus on whether “an AI technology determines the expressive elements of its output” and the “extent to which the human had creative control over the work’s expression and actually formed the traditional elements of authorship” (88 Fed. Reg. 51, 16193 (2023)). The Copyright Office also explicitly warned that copyright applicants have a “duty to disclose the inclusion of AI-generated content in a work submitted for registration and to provide a brief explanation of the human author’s contributions to the work” (88 Fed. Reg. 51, 16193 (2023)).

The Copyright Office has published on its website four decisions already issued by its review board (the “Review Board”) on claims involving AI generated works: (1) a decision issued February 14, 2022 regarding the refusal of a claim for autonomously created two-dimensional artwork; (2) a decision issued on February 21, 2023 regarding the cancellation of a registration on a comic book which included content generated by AI; (3) a decision issued on September 5, 2023 regarding the refusal of a claim for two-dimensional artwork which included content generated by AI; and (4) a decision issued on December 11, 2023 regarding the refusal of a claim for two-dimensional artwork created by an AI software. The decisions were consistent with the principles defined by the Copyright Office in its recent guidance.

The Review Board's February 14, 2022 decision involved the refusal of registration on Steven Thaler's two-dimensional artwork claim in the work titled "A Recent Entrance to Paradise" (Thaler (Copyright Rev. Bd. Feb. 14, 2022)). In this case, the author of the work was identified as the "Creativity Machine," Thaler was listed as the claimant, and a note was left for the agency stating that the work was "autonomously created by a computer algorithm running on a machine" and he was "seeking to register this computer-generated work as a work-for-hire to the owner of the Creativity Machine" (Thaler, 2-7 (Copyright Rev. Bd. Feb. 14, 2022)). The Review Board affirmed the agency's decision to refuse registration of the copyright claim in the work on the grounds that Thaler provided no evidence that the work was the "product of human authorship" nor to convince the Office to depart from established copyright jurisprudence that "a work must be created by a human being." The Review Board also rejected an argument by Thaler that AI can be an author under copyright law because the work for hire doctrine allows for "non-human, artificial persons such as companies to be authors" on the ground that work-for-hire is created as a result of a "binding legal contract—an employment agreement or a work-for-hire agreement" and does not invalidate the requirement that a work be created by a human. The Review Board specifically noted that Thaler had not asserted that the work "was created with contribution from a human author" so that particular issue had not been presented to the Review Board for consideration.

The Review Board's February 21, 2023 decision involved Kristina Kashtanova's registration of her comic book work titled "Zarya of the Dawn" (Kashtanova (Copyright Rev. Bd. Feb. 21, 2023)). In this case, Kashtanova had obtained a copyright registration in the work on

September 15, 2022 and then the Copyright Office learned from subsequent social media posts she made thereafter that she had created the comic book using Midjourney AI (Kashtanova, 2-3 (Copyright Rev. Bd. Feb. 21, 2023)). The original application had not disclosed any use of AI in creating the work, and the claim had not been limited to any portion of the work. The Review Board concluded that the registration certificate was issued based on "inaccurate and incomplete information," which if known, would have resulted in the Copyright Office "[narrowing] the claim to exclude material generated by artificial intelligence technology" (Kashtanova, 12 (Copyright Rev. Bd. Feb. 21, 2023)). Accordingly, the Review Board stated it would cancel the previous registration and replace it with a new registration that covered only the original authorship contributed to the work by Kashtanova, which was "text" and "selection, coordination, and arrangement of text created by the author and artwork generated by artificial intelligence."

The Review Board's September 5, 2023 decision involved Jason Allen's two-dimensional artwork claim in the work titled "Théâtre D' Opéra Spatial" (Allen, (Copyright Rev. Bd. Sept. 5, 2023)). In this case, Allen had not disclosed in his application that the work was created using an AI system; however, the work had received "national attention for being the first AI-generated image to win the 2022 Colorado State Fair's annual fine art competition," which was known by the Copyright Office (Allen, 2 (Copyright Rev. Bd. Sept. 5, 2023)). The Copyright Office inquired by email about the application and the publicity regarding his win, and Allen disclosed that the work was created by the input of "numerous revisions and text prompts at least 624 times to arrive at the initial version of the image," which he then edited using Adobe Photoshop. The Review Board determined that upon a review of the application, the deposit and the correspondence from Allen, the work contained "an amount of AI-generated material that is more than *de minimis* and thus must be disclaimed" and that the work was "not the product of human authorship" (Allen, 3-9 (Copyright Rev. Bd. Sept. 5, 2023)).

Finally, the Review Board's December 11, 2023 decision involved Ankit Sahni's two-dimensional artwork claim in the work titled "SURYAST" (Sahni (Copyright Rev. Bd. Dec. 11, 2023)). In this case, Sahni listed two authors: himself as the author of the "photograph, 2-D artwork" and an AI software as the author of "2-D artwork" (Sahni, 2 (Copyright Rev. Bd. Dec. 11, 2023)).

The Copyright Office inquired by email regarding the application, and Shani responded with a 17 page document explaining how the technology functions and how he used the technology to create the work. The Review Board determined that the work did not "contain sufficient human authorship necessary to sustain a claim to copyright," since the "expressive elements of pictorial authorship" were provided by the AI tool rather than Sahni (Sahni 3-9 (Copyright Rev. Bd. Dec. 11, 2023)).

The Risk that the Use of AI will result in the Loss of Confidential Information and/or Trade Secrets

The third and perhaps most significant legal risk that organizational consultants and managers will encounter due to AI use is the risk that the use of AI will result in the loss of confidential information or trade secrets. The specific concern is that an individual, whether employee or independent contractor, will utilize a publicly available AI platform and prompt the platform with inputs of confidential information or even trade secrets that the AI platform then trains its data on. Thereafter, this confidential information or trade secrets then may potentially be exposed to subsequent users of the platform, resulting in a data breach, a lost trade secret, and/or other ethical, privacy, or contractual violations. Another concern is that confidential information or trade secrets exposed to the AI platform may be lost in a subsequent security incident involving the AI platform itself, resulting in a data breach that may include the exposed confidential information or trade secrets.

This risk is more than just a theoretical risk, and it is increasing as AI platforms are more widely adopted. A recent report by Menlo Security reported that over a sample size of 500 global organizations in a 30 day period, there were over 2.5 million visits to generative AI sites by some 78,825 users averaging about 32 times per month per user; 10,190 file upload events and 3,394 copy and paste events; and of the data imported during that window, the most commonly imported data was personally identifiable information, followed by confidential information (Menlo Security, 2024). A separate report by Netskope Threat Labs found that an "organization can expect around 660 daily prompts to Chat GPT for every 10,000 users, with source code being the most frequently exposed type of sensitive data. . .generating, on average 158 incidents monthly. . . . [followed by] regulated data (on average, 18 incidents), intellectual property (on average, four incidents), and posts containing passwords and keys (on average, four incidents) every month" (Passeri, 2023).

In fact, at least one technology company has been widely reported to have already suffered this type of security incident. Samsung Electronics semiconductor business unit suffered three separate data leaks involving Chat GPT: in the first incident, an employee uploaded faulty source code to obtain a solution; in the second incident, an employee entered "program code for identifying defective equipment to get code optimization; and in the third incident, an employee uploaded a converted audio file of a company meeting to convert the meeting into meeting minutes (Wilkinson, 2023). As a result of the incidents, Samsung Electronics is reported to have banned the use of ChatGPT and other generative AI platforms by employees (Petkauskas, 2023; Dreibelbis, 2023). It has been reported that other large companies like Apple, JP Morgan, Verizon and Amazon have taken the same approach and instituted similar bans of generative AI platforms by employees over concerns about the risk of potential leaks of sensitive company information (Vincent, 2023).

AI security incidents involving data breaches are also increasing. A survey by the AI Threat Landscape Report 2024 reported that 77% of businesses suffered a breach to their AI in

2023 (Cawley, 2024). It was also recently reported that thousands of servers had been compromised in the past year due an unpatched vulnerability in a particular open source computing framework used by AI and machine learning platforms (Constantin, 2024). Experts are anticipating that AI security threats will continue to expand as the technology continues to develop and adoption becomes more widespread.

Managing the Legal Risks of AI Use to IP and Confidential Information

Obviously, effective management of the legal risks of AI use to IP and confidential information requires more than just knowing about and understanding the risks: it also requires the adoption and implementation of certain AI management best practices to reduce and mitigate the risks of exposure to liability.

Limit Reliance on Generative AI

First and foremost, an initial best practice that all consultants and organizations should adopt and implement is a policy limiting reliance on generative AI to the development of ideas, the consideration of alternative options or positions, or general research, as opposed to relying on generative AI for the development of IP. As previously discussed, ideas alone do not constitute intellectual property unless they rise to the level of a trade secret or an invention; however, for the reasons previously discussed, any IP developed using AI poses an inherent risk of potentially infringing third party intellectual property. So, the safest practice for consultants and organizations is to refrain altogether from relying on generative AI to develop IP.

Notwithstanding the foregoing, reliance on the use of generative AI to develop IP is going to be less risky in certain narrow circumstances, which consultants or organizations may elect to permit on a limited basis. For example, if content developed through the use of generative AI is created solely for internal use only, or a logo or an image developed through the use of AI has been subjected to separate trademark or image clearance searches and advance approval to use was provided, then consultants or organizations may find such logo or image acceptable to use, even if developed through generative AI. In any such approved case, the consultant or organization should document for internal recordkeeping purposes how AI was used and what AI was used and should refrain from identifying the AI-developed work as original work. Also, to the extent that protection under U.S. Patent or Copyright Law is desirable for any such AI developed work, the use of AI should be minimized, in order to ensure that any contributions by the AI are minor and insignificant to what is developed. This will increase the likelihood that the intellectual property developed will in fact be protectable under U.S. Patent or Copyright Law.

Prohibit Uploads of Confidential, Proprietary, Sensitive or Personal Information to Non-Private Generative AI Platforms

Another best practice that should be implemented is to adopt a policy expressly prohibiting the upload of documents or files containing confidential, proprietary, sensitive, or personal information to generative AI platforms, except to the extent that the generative AI platform to which the document is being uploaded is a private rather than public AI platform. Unlike the commonly available public AI platforms, which are broadly available to a public audience, private AI platforms “operate in closed, restricted environments” and limit access to specifically authorized persons or entities. (Simpson). Essentially, a private AI is a private and secure generative AI that is fine-tuned and trained with the proprietary data of a business without being connected to the public generative AI. (Betts, 2023). Private AI may be implemented on a private server or in a public cloud that is privately walled; however, the key features of a private AI are that data management remains under the control of the business; there is a reliance on a decentralized processing model in lieu of the centralized processing model of public AI; and technology is utilized to ensure the privacy and security of sensitive data.(Datacenters.com, 2024).

Prohibit Integration or Use of Generative AI Tools Without Prior Authorization

A third best practice that should be implemented is to expressly prohibit the integration of generative AI tools into or with business software and prohibit the use of generative AI tools altogether, without prior review and authorization by consultant or the decisionmaker for the organization as appropriate. This enables the decisionmaker to have the opportunity to test a proposed generative AI tool in advance of use, and to make a determination as to whether or not such tool will potentially have access to confidential, proprietary, sensitive, or personal information. To the extent that a determination is made that integration of the tool into software for the business is likely to result in unauthorized third-party disclosures, then the consultant or organization then has the opportunity to block the integration before it takes place. Alternatively, if no such determination is made, the integration can proceed with the assurance that use of the tool or software is unlikely to result unauthorized disclosures of confidential, proprietary, sensitive, or personal information.

Segregate Business and Personal Generative AI Accounts

A fourth best practice that should be implemented is to require the utilization of separate generative AI accounts for business purposes only whenever generative AI is accessed for the business, and to expressly prohibit the use of personal generative AI accounts altogether in connection with the business. Enforcing a clear separation between business and personal accounts better segregates the business account from inadvertent disclosures of confidential, proprietary, sensitive or personal information that might subsequently result in an unauthorized third-party disclosure of such information.

Develop and Adopt AI Policy

A fifth best practice that should be implemented is to require the development and adoption of an AI policy for the business that incorporates and memorializes the foregoing requirements, along with any other AI practices and policies that are subsequently adopted and any penalties for non-compliance. Once adopted, adherence to the AI policy in effect should become a requirement for all employees and independent contractors working with the consultant or organization.

Incorporate Terms into Contracts Requiring Compliance with AI Policy

A sixth best practice that should be implemented is to require the incorporation of terms and conditions into all contracts, which require compliance with the then-current AI policy; warrant and represent that the party will comply at all times with the then-current AI policy; and indemnify, defend and hold harmless the business for losses and liabilities of any type that arise from any failure to comply with the then-current AI policy. By routinely incorporating these AI-related terms and conditions into all contracts, the AI policy is not only clearly communicated to third parties as a clear requirement for doing business with but then it also becomes an established business standard by which all vendors and other business partners are held to with regard to the use of AI in their businesses.

Develop and Adopt Training Program on Managing Legal Risks of AI

Finally, a seventh best practice that should be implemented is to develop and adopt a training program on managing the legal risks of AI, and to then require periodic attendance at that training program by all employees, independent contractors, vendors, and business partners. To facilitate compliance, the program should be made available as a videoconference or in an on-demand format. The content of any such training program should not only include education about IP and confidential information generally but also should include updates on the emerging risks of AI to IP and education on the then-current AI policy adopted by the consultant or organization. Finally, as a further resource, the consultant or organization should consider creating a virtual helpline to answer questions related to the training program or emerging legal risks of AI generally as those questions arise. The availability of educational resources and ongoing support will provide additional mitigation of the legal risks of AI for consultants and organizations alike.

Conclusion

All in all, the best strategy to mitigate the legal risks of AI to IP is to stay informed and keep employees, independent contractors, vendors, and businesses similarly informed as to emerging risks and concerns of AI on IP, while also developing common-sense practices and procedures to respond to and contain the risks as they evolve. Through this multi-layered approach, consultants and organizations can safely utilize AI technology without falling victim to its pitfalls.

References

Allen (Copyright Rev. Bd. Sept. 5, 2023).

Appel, G., Neelbauer, J., and Schweidel, D. (2023, April 7). Generative AI Has an Intellectual Property Problem. *Harvard Business Review*. https://hbr.org/2023/04/generative-ai-has-an-intellectual-property-problem.

Betts, Bryan. (2023, Nov. 18). Understanding the rise and role of Private AI. *Computer Weekly.com*. https://www.computerweekly.com/blog/Write-side-up-by-Freeform-Dynamics/Understanding-the-rise-and-role-of-Private-AI.

Brittain, B. (2024, Jan. 2). How copyright law could threaten the AI industry in 2024. *Reuters*. https://www.reuters.com/legal/litigation/how-copyright-law-could-threaten-ai-industry-2024-2024-01-02/.

Brittain, B. (2023, Jan. 17). Lawsuits accuse AI content creators of misusing copyrighted work. *Reuters*. https://www.reuters.com/legal/transactional/lawsuits-accuse-ai-content-creators-misusing-copyrighted-work-2023-01-17/.

Caldwell, K. (2023, October 23). AI and Intellectual Property: Who Owns It, And What Does This Mean for the Future? *Forbes*. https://www.forbes.com/sites/forbesbusinesscouncil/2023/10/31/ai-and-intellectual-property-who-owns-it-and-what-does-this-mean-for-the-future/?sh=1c2f078a3e96.

Cawley, C. (2024, March 22). Study: 77% of Businesses Have Faced AI Security Breaches. *Tech.co.* https://tech.co/news/study-business-ai-security-breaches.

Constantin, L. (2024, March 28). Thousands of servers hacked due to insecurely deployed Ray AI framework. *CSO Online.* https://www.csoonline.com/article/2075540/thousands-of-servers-hacked-due-to-insecurely-deployed-ray-ai-framework.html.

Datacenters.com. (2024, Feb. 16). The Benefits of Private AI for Organizations. https://www.datacenters.com/news/the-benefits-of-private-ai-for-organizations.

Dreibelbis, E. (2023 May 2) Samsung Bans ChatGPT After Engineers Use it to Fix Proprietary Code. *PC Mag.* https://www.pcmag.com/news/samsung-bans-chatgpt-after-engineers-use-it-to-fix-proprietary-code.

Kashtanova (Copyright Rev. Bd. Feb. 21, 2023).

Menlo Security (2024). *How employee usage of generative AI is impacting organizational security*. https://resources.menlosecurity.com/reports/how-employee-usage-of-generative-ai-is-impacting-security-posture.

Moreno, E. (2023, Dec.30). Boom in A.I. Prompts a Test of Copyright Law. *New York Times*. https://www.nytimes.com/2023/12/30/business/media/copyright-law-ai-media.html.

Passeri, P (2023, Aug. 16). The Risk of Accidental Data Exposure by Generative AI is Growing. Infosecurity Magazine. https://www.infosecurity-magazine.com/blogs/accidental-data-exposure-gen-ai/. (*Citing* Netskope Threat Labs (2024). *Cloud and Threat Report 2024*. https://www.netskope.com/netskope-threat-labs/cloud-threat-report/cloud-and-threat-report-2024.)

Petkauskas, V. (2023, May 9). Lessons learned from ChatGPT's Samsung leak. *Cybernews*. https://cybernews.com/security/chatgpt-samsung-leak-explained-lessons/.

Sahni (Copyright Rev. Bd. Dec. 11, 2023).

Simpson, Julie. Private AI vs. Public AI: What's the Difference? *Ronin Consulting.* https://www.ronin.consulting/artificial-intelligence/private-ai-vs-public-ai/.

Thaler (Copyright Rev. Bd. Feb. 14, 2022).

United States Copyright Office (2024, May 31). Circular 1 Copyright Basics by the Copyright Office. Retrieved May 31, 2024 from https://www.copyright.gov/circs/circ01.pdf.

USPTO (2024, May 31). Glossary. Retrieved May 31, 2024 from https://www.uspto.gov/learning-and-resources/glossary. Patent Basics. Retrieved May 31, 2024 from https://www.uspto.gov/patents/basics/essentials#questions. Trademark

Basics. Retrieved May 31, 2024 from https://www.uspto.gov/trademarks/basics/maintaining registration. Trade Secret Policy. Retrieved May 31, 2024 from https://www.uspto.gov/ip-policy/trade-secret-policy.

Vidal, K (2024, Feb. 12). AI and inventorship guidance: Incentivizing human ingenuity and investment in AI-assisted inventions. Director's Blog. https://www.uspto.gov/blog/ai-and-inventorship-guidance-incentivizing.

Vincent, J. (2023, May 19). Apple restricts employees from using ChatGPT over fear of data leaks. *The Verge.* https://www.theverge.com/2023/5/19/23729619/apple-bans-chatgpt-openai-fears-data-leak.

Wiggers, K. (2023, Jan. 27). The current legal cases against generative AI are just the beginning. *Tech Crunch*. https://techcrunch.com/2023/01/27/the-current-legal-cases-against-generative-ai-are-just-the-beginning/.

Wilkinson, L. (2023, April 7). Samsung employees leaked corporate data in ChatGPT: report. *CIO Dive*. https://www.ciodive.com/news/Samsung-Electronics-ChatGPT-leak-data-privacy/647137/.

17 U.S.C. §§ 106, 302, 408-412 (2022).

35 U.S.C. §§ 154, 173 (2024).

89 Fed. Reg. 30, 10045-10050 (2024).

89 Fed. Reg. 51, 16190-16194 (2023).