ARNON
ARNON, TADMOR-LEVY

Legal considerations for companies using AI - Article #2

Recently there has not been a day that goes by when we are not asked by concerned clients about the legal ramifications of using AI tools such as Chat GPT by Open AI, Co-Pilot by GitHub, or Vertex AI by Google. In the previous installment of this series, we outlined various legal frameworks that may govern the use of AI. This article is intended to provide some more practical steps that companies can take in order to account for legal considerations when using third-party AI tools.

As this field is still in its early stages of development and there is quite a bit of uncertainty as to how courts and regulators may approach the relevant issues, we will continue to develop these recommendations and publish updates periodically. If you would like to receive our updates directly, you are invited to sign up here.

When using third-party AI tools, we advise taking the following steps:

1. Review of Legal Documentation.

Legal documentation ("Terms") of third-party generative AI tools should be reviewed to understand the legal protections and exposures. While these Terms may look similar, there are nuances that are important to consider, such as those regarding ownership of intellectual property and privacy matters. We recommend checking the relevant Terms from time to time as these documents may be updated and you may not be notified of an update.

2. Paid Services.

Various third-party tools are available either as a free version or as a paid, enterprise service. In general, the legal protections around the paid services are more robust than those in the free versions. For example, paid services may not use the data you input to train the third-party AI algorithm further, which would decrease risks related to intellectual property, privacy, and data protection.

3. Protection of Your Data Input.

Be sure to understand what rights the third party has to the materials you input to the tool. Verify whether you have the right to provide the data (ownership, privacy) and how the third party will use the data. For example, does the third party get the right to use the data you input to continue to train its systems? In general, it is not advisable to input any sort of trade secrets, personal data, or other highly confidential information.

4. Ownership of Output.

Make sure you understand whether you will own the materials generated by the third-party AI tool and whether the third party retains any rights to this output. Be sure that the ownership regime aligns with your intended use. For example, if you plan to sell the generated materials, you will need to have full, sole ownership of the materials and not only a limited license to use. This issue may be critical in connection with a financing round or M&A when the investor or purchaser would require the company to represent that it owns all of its intellectual property. Ensuring your ownership rights at the beginning may save you from a lot of issues at later stages.

5. Warranties and Indemnities.

Third-party tools rarely provide any legal guarantees or protections around the quality or non-infringement of the materials generated, which involves some risk that an unrelated third party may claim ownership over the materials generated. By further modifying the generated materials before using them, you may gain some protection against a claim that the generated materials you are using infringe the rights of a third party. If the use of generated materials is extensive, you may want to conduct a search for existing patents and copyrights that may be relevant to the code.

6. Privacy.

Companies offering AI tools are not always transparent about their use of personal data. If you will be providing any personal data to be processed by a third-party AI tool, make sure that you have the right to provide this data in accordance with applicable law. Do not input personal data to the system if it is not necessary to do so. Where possible, implement appropriate security measures to protect data collected by such platforms, such as encryption, access controls, and monitoring (i.e. on-prem use is safer than cloud-based).

7. Monitor and Record Your Use of AI Tools.

The widespread adoption of these AI tools is likely to grow across various segments. We already see uses by R&D, business development, marketing, financial, and legal teams. We encourage companies to keep records of the use of these tools across departments and to track which tools have been used, for what needs, and what the outcome of these uses was. Monitoring will allow management and legal teams to evaluate the risks across the company and to take necessary steps when there are regulatory or legal developments, which is important as the user or organization using the third party tool will be liable for any use of the tool.

8. Commercial Agreements.

Consider including a disclaimer regarding your use of AI and where a third-party AI tool you use disclaims warranties, ensure that you have back-to-back disclaimers in your commercial agreements. In addition, ensure you have contractual protections vis-à-vis customers in connection with potential IP infringement issues.

9. Transparency.

Be transparent about your use of AI to your customers and investors.

10. Risk Management.

For risk management purposes, consider adopting an AI risk mitigation policy, based on an assessment of the risk of the AI tools used by your organization. From a legal perspective, the fact that exposures were considered and that reasonable steps were taken to mitigate exposures may have benefits when facing external claims even in light of uncertain environment.

The above recommendations are intended to help companies mitigate some risks, though they will not eliminate risks entirely. Early implementation of a risk mitigation policy which includes all or parts of the aspects which described above is a good place to start.

For further information on this topic please contact Netanella Treistman, Roy Keidar or Derora Tropp at Arnon, Tadmor-Levy by telephone (+972 3 684 6000). The Arnon, Tadmor-Levy website can be accessed at www.arnontl.com.

Roy Keidar, Partner
Emerging Technologies
RoyK@ArnonTL.com

Netanella Treistman, Partner
Technology and Privacy
NetanellaT@ArnonTL.com

Derora Tropp, Associate
Technology and Privacy
DeroraT@ArnonTL.com