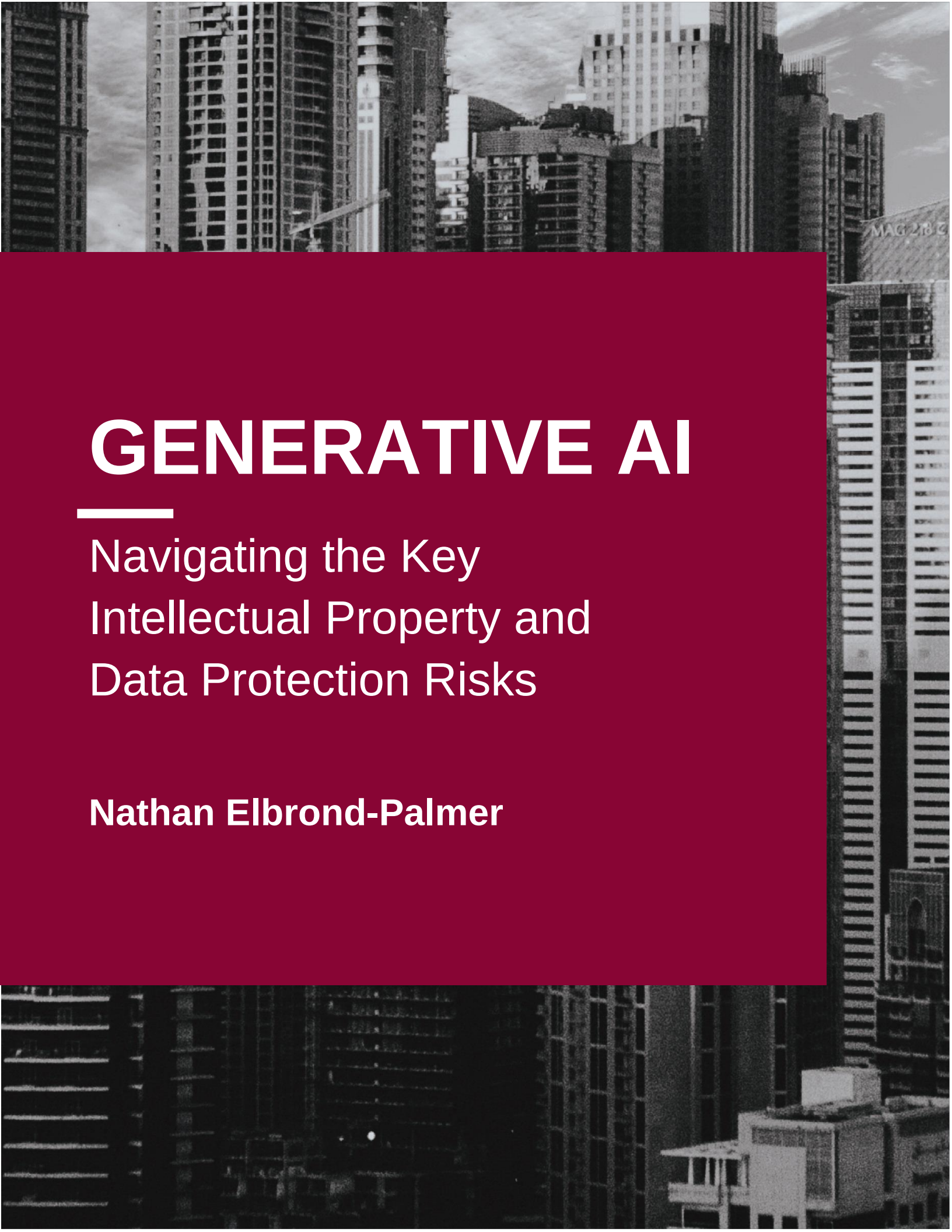

GENERATIVE AI

Navigating the Key Intellectual Property and Data Protection Risks

Nathan Elbrond-Palmer

Introduction

In a world characterised by increasing geopolitical tensions, macroeconomic shocks and general after-effects of a destructive pandemic, disruption has arguably been a common thread over the last twelve months. More recently, the disruptive power of artificial intelligence (AI) has once again resurfaced, with the emergence of chatbots such as ChatGPT and image generators like DALL-E 2. Whether it be new images, text or software code, these tools are all instances of generative AI, which refers to algorithms that can be used to generate new content of some kind. As with any innovative new technology with such powerful capabilities, generative AI has created a myriad of novel risks from a legal standpoint. This note focuses in on two of these major risk categories, namely Intellectual Property and Data Protection concerns, as well as exploring how stakeholders can reduce their exposure and maximise the associated benefits.

Intellectual Property Risk

i) Copyright infringement

The risk of potential copyright infringement has been at the very forefront of IP concerns raised regarding the emergence of generative AI. Simply put, the infringement risk flows from the possibility that an AI algorithm may copy copyright material which is then recognisable in the output it generates. At their core, generative AI algorithms such as ChatGPT are trained through machine learning, which involves exposing the algorithm to large datasets of text and other materials from the internet.[1] In some cases, these datasets may include materials subject to copyright protection, creating the risk that the algorithm's output could be similar or even identical to works already in existence.[2] Whilst direct copyright infringement claims would potentially arise in relation to copyright material being recognisable in the output, there is equally the potential for indirect claims, where the output generated does not itself contain a copy of the input but where the input was nevertheless used unlawfully. When scraping data for use in the machine learning process, AI developers should therefore take various steps to manage this infringement risk; this could involve excluding copyright material from the dataset entirely or alternatively obtaining permission from the owners of such material, perhaps through obtaining a valid licence.

Failure to pursue such pre-emptive actions may have significant detrimental consequences, increasing the litigation risk faced by AI developers. For instance, stock photo provider Getty Images recently brought a copyright infringement claim against artificial intelligence company Stability AI Inc, alleging that millions of its images had been copied without their consent and used to train Stability's text-to-image AI model.[3] In this particular case, some of the images produced by Stability's system in fact included distorted versions of the Getty Images watermark.[4] As such, Getty claims that Stability has infringed on its copyright by failing to obtain an adequate licence before copying the images in question.[5]

From a different perspective, AI developers may well attempt to argue that their usage of copyright works without permission could be allowed under the fair dealing exceptions under English copyright law. Indeed, in accordance with Sections 29 and 30 of the Copyright, Designs and Patents Act 1988 (CDPA), fair dealing may act as a legitimate defence if: (i) the use is for the purposes of research or private study, (ii) the use is for the purposes of criticism, review or quotation, or (iii) where the copyright work is utilised for the purposes of reporting current events.[6] Pending judicial clarification on the subject, it remains to be seen whether AI developers will be successful in relying on these fair dealing exceptions. For now, the very fact of Getty Images'

[1] Charlie Burrell & Mark Cusack, *Generative AI's copyright conundrum,* MACFARLANES LLP (Feb. 20, 2023), https://blog.macfarlanes.com/post/102i82d/generative-ais-copyright-conundrum

[2] Matt Hervey, *AI and copyright in 2022*, GOWLING WLG (Jan. 25, 2023), https://loupedin.blog/2023/01/ai-and-copyright-in-2022/#page=1

[3] Getty Images Staff, *Getty Images Statement*, GETTY IMAGES (Jan. 17, 2023), https://newsroom.gettyimages.com/en/getty-images/getty-images-statement

[4] Mark Nichols, *Getty images launches litigation against Stability AI over alleged misuse of images*, POTTER CLARKSON LLP, (Jan. 18, 2023), https://www.potterclarkson.com/insights/getty-images-launches-litigation-against-stability-ai-over-alleged-misuse-of-images/

[5] Getty Images Staff, *Getty Images Statement*, (n 3).

[6] Copyright, Designs and Patents Act 1988 (CDPA 1988) Section 29-30.

claim and the emergence of litigation in this field underlines that the risk for AI developers is an increasingly practical one, rather than simply being theoretical.

It is also important to note that, until very recently, developers had been set to benefit from the UK government's proposal to extinguish this copyright infringement risk altogether through introducing a text and data mining (TDM) exception to copyright law. Under this proposal, the fair dealing exceptions noted above would have been expanded to include text and data mining for commercial purposes, whereas the existing TDM exception under UK law is limited to purely non-commercial research.[7] Simply put, this change would have enabled AI developers to train their AI models using copyright-protected works without any risk of copyright infringement, forgoing the need to obtain consent or a valid licence from the owners. Importantly, however, the government's proposal was shelved in February 2023 in the face of a backlash from content creators.[8] Therefore, the risk for developers ultimately remains for the time being and the court's determination in the Getty Images dispute will be much-awaited.

ii) Can copyright subsist in the output of generative AI algorithms?

Before turning to the issue of whom exactly owns the copyright in the output, it is worth briefly meditating on the issue of whether or not the output generated by the AI may even qualify for copyright protection in the first place. In order to benefit from such protection, the output must meet a certain threshold of originality and authorship of the work must be attributed.

As per Section 1(1) of the CDPA, copyright may only subsist in "original… artistic works".[9] At this stage, it remains unclear whether a user inputting a specific text prompt into a generative AI algorithm would satisfy this originality requirement. Originality has, according to the English courts, generally been satisfied where an author has applied their own judgement, skill and individual effort, and has not copied the work.[10] Whilst the scope of this note does not extend to a detailed discussion of whether or not AI-generated works do in fact meet this originality threshold, this issue continues to be the subject of academic debate.[11]

Even in circumstances where the originality threshold has been reached, different jurisdictions have come to different conclusions regarding the authorship question which inevitably follows. For example, the US Copyright Office recently ruled that images created by the image-generator Midjourney in response to a human's text prompts were not copyrightable as they were "not the product of human authorship."[12] By contrast, in the UK the CDPA confirms that copyright can in fact subsist in a work generated by a computer in instances where there is no human author. Indeed, section 9 of the CDPA clarifies that the 'author' of these works under the law will be the person "by whom the arrangements necessary for the creation of the work are undertaken."[13]

iii) Who owns the copyright in the end product?

In terms of determining ownership, the author is generally regarded as the first owner of the copyright under UK law, meaning that determining the author becomes decisive in determining the relevant owner. Whilst very few cases have explored authorship under section 9, in one such case it was held that a person who took screenshots

[7] *Artificial Intelligence and Intellectual Property: copyright and patents: Government response to consultation*, THE INTELLECTUAL PROPERTY OFFICE OF THE UNITED KINGDOM (June 28, 2022), https://www.gov.uk/government/consultations/artificial-intelligence-and-ip-copyright-and-patents/outcome/artificial-intelligence-and-intellectual-property-copyright-and-patents-government-response-to-consultation

[8] Rachel Montagnon & Sungmin Cho, *UK withdraws plans for broader Text and Data Mining (TDM) copyright and database right exception*, HERBERT SMITH FREEHILLS LLP (March 1, 2023), https://hsfnotes.com/ip/2023/03/01/uk-withdraws-plans-for-broader-text-and-data-mining-tdm-copyright-and-database-right-exception/#page=1

[9] Section 1(1) CDPA 1988

[10] Theo Savvides & Sean Ibbetson, *Brexit and copyright law: will the English courts revert to the 'old' test for originality?* WOLTERS KLUWER (Dec. 5, 2016), https://copyrightblog.kluweriplaw.com/2016/12/05/brexit-copyright-law-will-english-courts-revert-old-test-originality/

[11] Matt Hervey & Matthew Lavy, *The Law of Artificial Intelligence*, SWEET & MAXWELL (15 Dec. 2020), 8-137.

[12] Cerys Wyn Davies, *Midjourney decision intensifies questions over definition of 'human authorship'* PINSENT MASONS LLP (March 10, 2023), https://www.pinsentmasons.com/out-law/analysis/midjourney-decision-intensifies-questions-definition-human-authorship

[13] Section 9 CDPA 1988

whilst playing a computer game was not the author of the screenshots in question.[14] Instead, it was held that the game's developers had undertaken the arrangements necessary for the creation of the images.[15]

Applying the logic of this ruling to generative AI could have the following impacts. Firstly, there might be an expectation that, where human input in the generation of the output is more minimal, and where the creation of the work mostly arises from automated decisions taken by the AI algorithm, the authors of the output would be the platform creators. Conversely, where human users exercise a significant degree of input and control through their prompts, with the AI platform acting merely as a tool for the human user, the argument for the human user as the author appears to be more persuasive.

Whilst the foregoing discussion suggests that, in many instances, the platform creator may be the first owner of the output by operation of law, several creators' terms of use explicitly assign the rights to the generated output to the users themselves. This includes creators such as Github[16], which developed the Copilot service for generating new code, as well as OpenAI[17], which has developed a myriad of generative AI products including ChatGPT, DALL-E 2 and Whisper. In any case, it is crucial that users of generative AI products consult the relevant platform's terms of use to clarify the terms on which the output is being provided to the user contractually. For instance, there may be cases in which the output is not assigned upon creation, but instead provided to the user under a licence, which may very well include terms restricting how the output may be used.

This point is particularly significant for businesses who may rely on generative AI to produce project deliverables and intend to eventually transfer ownership of these deliverables to the end-client. Indeed, where the relevant AI platform's terms do not assign the IP to the output in the business, the business may face challenges in attempting to transfer ownership of the work onto the end-client.

Data Protection Risk

i) Personal Data

As explored during the earlier discussion of copyright infringement risk, generative AI algorithms rely on large datasets gathered from the internet combined with information provided by users themselves. As well as much of this information being subject to copyright protection, much of the information also relates to natural persons, meaning it qualifies as personal data and will therefore be subject to data protection law. As such, any personal data being processed must be used and protected in line with applicable data privacy and protection laws.

However, on the face of it, a number of these applicable laws may sit uneasily with the nature of generative AI. As an example, Article 5(1)(c) of the UK General Data Protection Regulation (UK GDPR) contains the so-called 'data minimisation' principle, which requires that organisations should only process the minimal amount of personal data needed to fulfil the business purpose.[18] This may naturally conflict with the reality that, often, the more data an AI system is trained on, the more statistically accurate the system becomes.

Notably, the ramifications of non-compliance in this area extend not only to punitive fines but also in some circumstances to the banning of entire services. As recently as February 2023, the Italian Data Protection Authority issued an order banning an AI-powered chatbot service from any further processing of Italian users'

[14] *Nova Productions Ltd v Mazooma Games Ltd* [2007] EWCA Civ 219
[15] Ibid
[16] *GitHub Terms for Additional Products and Features*, GITHUB (Nov. 3, 2022), https://docs.github.com/en/site-policy/github-terms/github-terms-for-additional-products-and-features#github-copilot ("The code, functions, and other output returned to you by GitHub Copilot are called "Suggestions." GitHub does not claim any rights in Suggestions, and you retain ownership of and responsibility for Your Code, including Suggestions you include in Your Code.")
[17] *Terms of Use*, Sec. 3(a), OPENAI (March 14, 2023), https://openai.com/policies/terms-of-use ("Subject to your compliance with these Terms, OpenAI hereby assigns to you all its right, title and interest in and to Output.")
[18] UK General Data Protection Regulation (UK GDPR) Article 5(1)(c)

data.[19] Central to the rationale for this order was the view that the service's privacy policy had failed to disclose the key elements of the personal data processing being performed, thus flouting the transparency principles and obligations set out in the GDPR.

It is important to emphasise that this particular risk may not always need to be managed solely by the platform creators themselves, but also potentially by the end users. This is particularly so in the case of ChatGPT, with OpenAI's terms of use clarifying that it is the user's responsibility to ensure that it has the right to process any personal data.[20] This means that users processing personal data must comply with several obligations as a data controller, including "providing legally adequate privacy notices"[21] and obtaining "the necessary consents for the processing of such data".[22] Ultimately, in order to comply with the applicable data protection laws, users sharing personal data and who are under the scope of GDPR must opt in to execute a Data Processing Addendum, which does not apply automatically.

As this foregoing discussion indicates, users of any generative AI products and services should rigorously consult the terms and conditions of these products, noting the allocation of risk and which party is required to ensure that personal data is being processed and protected in a compliant manner.

ii) Confidential Information

A further data protection risk for users of generative AI algorithms relates to the way in which these algorithms may utilise input and output data in order to continuously improve the services being provided. To return to OpenAI, for instance, their terms of use have stipulated that data ingested by ChatGPT may be used to develop and improve their services.[23] The corollary of this is that, depending on different platforms' specific terms, it is possible that information the user provides will not be kept confidential and may be viewed for research or training purposes by OpenAI's employees. In light of this, businesses should be circumspect about sharing information with these algorithms which may be subject to contractual confidentiality limitations, such as information relating to clients and customers.

Where possible, businesses sharing confidential information should attempt to opt-out of this practice of having their data used to improve the AI model. Moreover, risk can be reduced here by ensuring that inputs to such models are sufficiently limited in detail or abstract so as to protect confidentiality. Employers should also aim to guard against this issue by updating their employee confidentiality agreements and policies. For instance, employers could minimise their risk by updating policies to include prohibitions or restrictions on employees entering confidential, proprietary or trade secret information into AI chatbots.

Final Word

As stated at the outset, the disruptive potential of technology has once again been reaffirmed over the past six months, with generative AI algorithms being introduced to the public at large and gaining significant popularity overnight. Investment into the space has risen sharply, with Microsoft Corporation announcing a $10 billion investment into OpenAI in January 2023.[24] As a result, businesses are rapidly experimenting with the new platforms and exploring how their adoption might drive increased efficiencies and innovation. However, as with other cutting-edge technologies, novel legal issues have arisen and must not be overlooked. This note has explored two of these significant risk categories, namely Intellectual Property and Data Protection, and has

[19] Eleonora Curreli & Laura Liguori, *The Italian Data Protection Authority Blocks AI Chatbot Replika Due to Endangerment of Minors and Vulnerable People*, GLOBAL ADVERTISING LAWYERS ALLIANCE (March 2, 2023), http://blog.galalaw.com/post/102i95y/the-italian-data-protection-authority-blocks-ai-chatbot-replika-due-to-endangerme
[20] *Terms of Use*, Sec. 5(c), OPENAI (March. 14, 2023)
[21] Ibid
[22] Ibid
[23] *Terms of Use*, Sec. 3(c), OPENAI (March 14, 2023)
[24] Dina Bass, *Microsoft Invests $10 Billion in ChatGPT Maker OpenAI*, BLOOMBERG (Jan. 23, 2023), https://www.bloomberg.com/news/articles/2023-01-23/microsoft-makes-multibillion-dollar-investment-in-openai

provided suggestions for how these risks can be mitigated. Ultimately, the winners in this area will be those developers, businesses and users alike who can maximise the benefits of generative AI without exposing themselves to undue risk and liability.