The IP Protection of AI Inventions

Laurynas Adomaitis & Edward Hunter Christie

AI Policy Blog
5 July 2021

The authors review the main modes of defence and attack with respect to the Intellectual Property (IP) of AI inventions. We consider the defender to be the nation where the IP originates and the attacker to be a foreign nation or organization that seeks illicit access to it.

Corporate choices in the defender nation

In the general case, corporations choose between (or combine) two main approaches, patents and trade secrets, when seeking legal protection for distinctive ideas that underpin their products.

A patent is a 20-year monopoly granted to an inventor to make, use, and sell an invention, in exchange for a detailed description of the invention being published [1]. Under the European Patent Convention (EPC), the invention must be new, involve an inventive step, and be industrially applicable [2]. Very similarly, under US law, inventions must be new, non-obvious, and useful (where usefulness includes not only having a useful purpose but also operativeness) [3, 4]. As a patent allows the inventor to license the use of the invention to others in exchange for license payments, or to choose not to provide licenses to certain competitors, it constitutes an economic incentive to apply for patents. For public policy, patent publication ensures the dissemination of innovative ideas, supporting further innovation. To protect this approach, unauthorised uses of patents are subject to penalties. To provide certainty to prospective patent holders, subsequent development by others of the same invention, whether independently or through reverse engineering, is considered an infringement and is subject to penalties [5].

Resorting to patents does not preclude a partial use of open-source licensing [6], whereby some software tools and their underlying code are released to the public. While open-source licensing means forgoing the licensing fees available through the patent regime, it can be part of a broader outreach strategy, supporting both customer acquisition and talent acquisition goals [7]. Patenting remains useful in this setting to preempt rival corporations patenting the same invention first, which would give them legal leverage [8].

The trade secrets approach is in a sense the mirror opposite of patenting. Under both US and EU law, a trade secret is information that is not generally known or discoverable by others, is maintained in secrecy by its owner, and gives its owner a competitive advantage because it is secret [9, 10]. Under the trade secrets approach, the owner is not protected from competitors developing the same idea independently or through reverse engineering [11, 12]. Effectively, trade secrets are only violated through theft. The owner's IP rights will be upheld in a court of law provided it is shown that reasonable steps were taken to preserve secrecy. Naturally, an innovation that is patented or open source cannot also be a trade secret.

The definition of trade secrets covers a broader scope and is easier to meet than what is required for a patent. Not coincidentally, estimates suggest that trade secrets are the dominant choice to protect inventions. This is not easy to ascertain: patent data is centralised in national patent offices and published whereas national data collection on trade secrets is an impossibility. However, analyses using proxy measures enable estimates of the share of inventions that are patented which could be as low as 10% [13]. This share is also found to vary substantially between industries and world regions, with rates in Asia higher than in Europe or North America [14].

While companies resort to a mix of patenting, open-source licensing, trade secrets, and copyright protection [15] for different parts of their IP, the trade secrets approach has become relatively more important in recent years. In an influential 2012 paper [16], David S. Almeling identified several reasons for that trend, including notably the rise of digital technologies, more mobile workforces, the rising value of intellectual property (of which trade secrets are a part), and an increase in international threats. In response to these trends, both the United States and the European Union adopted new, stronger, and mutually coherent legislation on trade secrets in 2016. In doing so, foreign IP theft was mentioned, more explicitly in the US context, but also through carefully referenced footnotes and case studies in the European Commission’s 2013 Impact Assessment [17] that accompanied the then-proposed legislation.

Does the general trend towards trade secrets also apply to Artificial Intelligence? For the United States, AI patent applications increased from 30,000 to 60,000 annually between 2002 and 2018 and the share of AI applications in total patent applications rose from 9% in 2002 to nearly 16% in 2018 [18]. However, these increases occurred while the entire field of AI was growing strongly on every available metric. Importantly, there is no available measure of the number of AI trade secrets. Analyses using proxy measures could help to estimate whether AI trade secrets have grown at a lower, equal, or higher rate than AI patents.

The attacker’s choices

From the attacker’s perspective, there are choices concerning the mode of access to the target’s IP and concerning responses to the target’s reaction in case the access is detected. Modes of access include analysing the information published by the target (including patent information), analysing marketed goods and services purchased from the target, stealing and analysing prototypes, short-term or long-term economic espionage through human or cyber infiltration, and remote model extraction attacks (which we treat as distinct from ordinary cyber espionage). If the attack is detected, the target may respond with a combination of resilience-enhancing measures and legal avenues. In response to the former, the attacker may switch to another mode of access or seek new ways of exploiting an existing mode of access. In response to the latter, the attacker may be able, depending on the jurisdiction, to count on weak or delayed enforcement or on political channels of influence to influence the legal process.

Most of the considerations above apply across technologies. For AI, there is also the threat of model extraction attacks, also referred to as replication attacks or model stealing [19, 20, 21]. If a Machine

Learning model is deployed, accessing data for further training and outputting prediction results, it is possible to design attacks that effectively query the model and use observable responses for the purpose of reverse engineering. Such attacks could be part of an IP theft strategy with commercial underpinnings. They could also constitute threats to national security if one envisages an adversary extracting the Machine Learning models used by the defender nation for security or defence purposes, or to manage important civilian functions such as critical infrastructure. In case of conflict, an attacker with knowledge of the defender's Machine Learning models would have foresight as to the actions the models will recommend or take under scenarios the attacker could simulate ahead of time. The attacker would also be far better able to mount attacks that succeed in misleading the defender's models into making self-defeating decisions and recommendations.

State choices in the defender nation

For public policy, the goal is to encourage useful innovations for general economic purposes as well as for defence and security purposes while ensuring that relevant sensitive information is protected accordingly, most notably from rival foreign states.

The defender nation can deploy a combination of information campaigns and legal obligations to ensure that corporate actors take adequate steps to protect their trade secrets. The three main categories to consider are physical security, cyber security, and legal measures such as confidentiality, non-compete, and non-disclosure agreements (NDAs) [23]. Public policy can strengthen the legal mechanisms available to corporations to obtain redress in case of IP theft, as has occurred already with the strengthening of trade secrets legislation. Legal obligations to ensure a minimum level of cyber-security, while addressing broader needs than just IP theft, are also conducive to this goal. States can also choose to make use of foreign policy instruments to seek to incentivise a reduction in foreign state-sponsored IP theft.

In parallel, states also subject defence- and security-sensitive inventions to state secrecy, with the companies and individuals involved prohibited from sharing relevant information and from distributing relevant goods and services to customers other than designated institutions. When this emerges from a prior relationship between the government sector and a company, the latter will have been previously required to obtain security clearances at company level and for key staff.

Most of the inventions that are subject to state secrecy seem to be generated in the defence industry ecosystem. One available proxy measure that suggests this pattern is the breakdown, between defence industry applicants and other applicants, for patents that become subject to state secrecy. In the United Kingdom, over the 2018-2019 period, a total of 11,930 patents were granted and 117 patents were subject to a national security prohibition [24]. Of those that were subject to secrecy, 94 (80%) were from defence industry applicants [25]. For the United States, over 2018 and 2019 combined, 173 new secrecy orders were issued [26], while the USPTO reports a total of 731,095 patents granted for that period [27]. So, while the ratio of secrecy orders to patent grants is around 1% in the UK, it is only 0.02% in the United States (about double if one excludes grants to foreign applicants). On the other hand, of the 173 new US secrecy orders, 91 (53%) were so-called "John Doe" cases, namely cases where the applicant was neither the government sector nor a contractor for the government sector. No further breakdown is available regarding these cases [28].

There is a clear public interest case for having national patent offices act, as they do currently, as gatekeepers for security-sensitive patent applications. However, from the overall indicators discussed above, the share of the patent system in security-sensitive IP is difficult to quantify. It may be quite limited in view of the generally greater role played by trade secrets and of the fact that state secrecy is superimposed on trade secrets in the common case where a prior relationship exists between the inventor and the government sector.

Effectively, there is a trade-off between patents and trade secrets and both approaches are conducive to innovation in different ways [29]. In the case of non-security sensitive IP, if the defender nation faces a changed international environment in which IP theft is potentially more impactful, a relative shift in favour of trade secrets would seem a rational response for most corporations. In any case, strengthening the ability of companies to be resilient seems a good way forward. For security-sensitive IP, state secrecy can operate with or without patents, and states have additional instruments at their disposal, notably export controls on military and dual-use goods, and intelligence and counterintelligence structures. Many challenges are common across technologies. In addition, the AI-specific challenge of model extraction attacks deserves particular attention, for both economic and national security reasons.

Many questions remain. Do existing legal and institutional approaches to IP provide the right incentives for the greater role of non-defence industry companies in desirable security-sensitive innovation that policy makers often call for? For example, should the compensation mechanisms relating to patent secrecy orders be more generous to elicit such innovation? Are new and stronger agreements among groups of like-minded nations necessary to better contain the actions of certain other states? Could a greater use of sanctions on designated individuals and entities in rival states [30] have an impact on the propensity to commit IP theft? We leave these questions open for future discussions.

How to cite this blog article (APA style):
Adomaitis, L. & Christie E. H. (2021, July 5). The IP Protection of AI Inventions. AI Policy Blog.

Notes

[1] https://www.wipo.int/patents/en/faq_patents.html
[2] https://www.epo.org/service-support/faq/basics.html
[3] https://www.uspto.gov/patents/basics
[4] In Article 27(1) of the TRIPS agreement, the European formulation is used with a footnote specifying that the US formulation may be deemed synonymous.
[5] Freibrun, Eric (1995, February 2). Intellectual Property Rights in Software – What They Are and How to Protect Them. Freibrun Law Blog.
[6] Calvin, N., & Leung, J. (2020). Who owns artificial intelligence? A preliminary analysis of corporate intellectual property strategies and why they matter. Future of Humanity Institute, February.

[7] Customer acquisition because users who are satisfied with an open-source tool may opt to pay for a more elaborate version or for accompanying services. Talent acquisition because software developer communities are stimulated to engage with the company's products (Calvin & Leung).

[8] Calvin & Leung

[9] 18 U.S.C. § 1839

[10] Directive (EU) 2016/943, Art. 2(1)

[11] Under US law, "improper means" of acquiring trade secrets "does not include reverse engineering, independent derivation, or any other lawful means of acquisition", see 18 U.S.C. § 1839.

[12] See Recital 16 of Directive (EU) 2016/943.

[13] Fontana, R., Nuvolari, A., Shimizu, H., & Vezzulli, A. (2013). Reassessing patent propensity: Evidence from a dataset of R&D awards, 1977–2004. Research Policy, 42(10), 1780-1792.

[14] Fontana et al. estimate 8.22% and 7.55% for the United States and Europe respectively, versus 25.13% for Asia.

[15] Copyright protection applies to the particular form in which an idea is expressed. For software, copyright law protects the source and object code, and certain unique original elements of the user interface (Freibrun)

[16] Almeling, D. S. (2012). Seven reasons why trade secrets are increasingly important. Berkeley Technology Law Journal, 1091-1117.

[17] European Commission (2013). SWD(2013) 471 final. (Footnotes 500 and 506, and Cases 6 and 14 in the text.)

[18] Toole, A., Pairolero, N., Giczy, A., et al. (2020). Inventing AI: Tracing the diffusion of artificial intelligence with US patents.

[19] For an overview of risks and threats to AI, see for example: Patel, Andrew; Hatzakis, Tally; Macnish, Kevin; Ryan, Mark; Kirichenko, Alexey (2019): D1.3 Cyberthreats and countermeasures. De Montfort University. Online resource. https://doi.org/10.21253/DMU.7951292.v3

[20] Orekondy, T., Schiele, B., & Fritz, M. (2019). Knockoff nets: Stealing functionality of black-box models. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 4954-4963).

[21] Jagielski, M., Carlini, N., Berthelot, D., Kurakin, A., & Papernot, N. (2020). High accuracy and high fidelity extraction of neural networks. In 29th {USENIX} Security Symposium ({USENIX} Security 20) (pp. 1345-1362).

[23] Kasdan, Michael J., Kevin M. Smith & Benjamin Daniels (2019, December 12). Trade Secrets: What You Need to Know. The National Law Review.

[24] This is termed a national security direction under Section 22 of the UK Patents Act 2004.

[25] See Table 1 and Table 2.8a, UK Intellectual Property Office (2020). Facts and figures: Patent, trade mark, design and hearing data: 2019.

[26] https://www.uspto.gov/web/offices/ac/ido/oeip/taf/reports.htm

[27] https://fas.org/sgp/othergov/invention/

[28] One may speculate a mix of new entrants to the defence industry who expected a secrecy order and others aiming at a commercially successful dual-use invention, wrongfooted by an unexpected secrecy order.

[29] While Gross (2019) finds that temporary secrecy orders during the Second World War had a permanent negative impact on later patent citations, this does not establish the trajectory of innovation embedded in trade secrets. On the other hand, Png (2017) finds that a shift towards trade secrets does not necessarily reduce innovation.

Gross, D. P. (2019). The consequences of invention secrecy: Evidence from the USPTO Patent Secrecy Program in World War II (No. w25545). National Bureau of Economic Research.

Png, I. P. (2017). Law and innovation: evidence from state trade secrets laws. Review of Economics and statistics, 99(1), 167-179.

[30] As suggested for example by Farley & Isaacs (2020, p. 152).

Farley, R. M., & Isaacs, D. H. (2020). Patents for power: Intellectual property law and the diffusion of military technology. University of Chicago Press.