Securing innovation in digital manufacturing supply chains: an interdisciplinary perspective on intellectual property, technological protection measures and 3D printing/additive manufacturing

Kwaku Adu-Amankwa* and Angela Daly

Introduction

In the Internet age, the relationship between IP and digital technologies has become the subject of intense debate, giving rise to legislative reforms, a vast body of case law and commercial and technical adaptations extensively

The authors

- Kwaku Adu-Amankwa is a PhD candidate at the University of Strathclyde, Glasgow, United Kingdom, based within the department of Design, Manufacturing and Engineering Management, and affiliated with the Centre for Internet Law & Policy. He researches complex security relationships associated with IP of additive manufacturing (3D printing) applications within digitally enabled/transformed supply chains. Angela Daly is a Professor of Law at the University of Dundee, Dundee, United Kingdom, jointly appointed by the Leverhulme Research Centre for Forensic Science and Dundee Law School. She conducts research across IP, data protection, competition and sector-specific regulation and human rights law.

Abstract

- Digital supply chains (DSCs) provide several advantages over traditional physical supply chains, yet they also pose new risks, including for IP, especially when associated with three-dimensional '3D' printing (3DP), also known as additive manufacturing (AM). Technological protection measure (TPM) usage in DSCs may help address the IP security issues of 3DP or AM but may result in overprotection and disregard for IP exceptions, which may also have a negative impact on innovation and other goals such as sustainability.
- This article considers how the IP security of 3DP/AM is addressed in DSCs, including by applying TPMs. We discuss whether the current approaches strike the right balance between the competing interests of different DSC actors.
- We also present some novel findings from a survey conducted with expert stakeholders to better understand IP security issues in practice. Our findings show that most respondents see IP and IP security efforts as both barriers and enablers to using 3DP/AM within DSCs. Also, the strategy chosen by most respondents for securing IP focuses on a technical approach, using inter alia TPMs. We infer that this dual perspective on IP and IP security may reflect the respondents' differing relationship with IP in DSCs, where one may wish to create, use and secure their own IP but also encounter barriers through the inaccessibility of the IP of third parties.

* Email: kwaku.adu-amankwa@strath.ac.uk. This paper contains research that is part of the lead author's PhD research project, supervised by a team including the second author, who contributed to the writing of this paper. The lead author's PhD research is supported by a scholarship from the University of Strathclyde. We want to thank the other members of the PhD supervision team: Andrew Wodehouse, Athanasios Rentizelas, Graeme McLaughlin and Jonathan Corney.

doi:https://doi.org/10.1093/jiplp/jpad062
Advance Access Publication 17 July 2023

documented in academic literature.[1] While most of the attention has focused on copyright, the interaction of digital technologies with other IP rights, such as trade marks and patents (eg for keyword advertising and software and hardware patents), has also attracted scrutiny.[2] Furthermore, questions over the ownership of data and trade secrets, data and algorithms also have IP-relevant aspects.[3]

As digital technologies, usually Internet enabled, have evolved, the debate has moved to new areas, including Internet-of-Things (IoT), artificial intelligence (AI) and smart manufacturing, especially three-dimensional '3D' printing (3DP) or additive manufacturing (AM). In many cases, these technologies give rise to interconnected issues, as they are deployed simultaneously, so that, eg a 3DP machine is part of the IoT.[4] These new technologies are also vehicles for IP creation and dissemination and, in some cases, IP overreach and present issues for securing and utilizing IP, increasing the complexity of the debate.

Digitalization facilitates decentralized manufacturing through a variety of technologies including 3DP, which relies on digital design files provided through digital communications means, such as the public Internet (especially for hobbyists using sites such as Thingiverse).[5] Larger industrial production using digital manufacturing may mobilize securer, private networks to send and receive files and other necessary information or data to produce objects.[6] In these ways, traditional supply chains, which previously typically involved centralized production in a large factory (often in China) and the distribution of products by sea, air and train, are transitioning to a different model, involving more decentralized and diffuse production, geographically closer to the end user.[7] The more traditional supply chain model experienced various IP security issues, such as copycat production, including in factories that may have produced legitimate versions of products by day and counterfeit versions by night.[8] However, digital supply chains (DSCs) may present more opportunities for IP infringement and, thus, reduce security for IP owners.

DSCs integrating 3DP offer advantages over conventional supply chains and centralized manufacturing in terms of increased sustainability, convenience and less wastage.[9] We have seen the tangible value of decentralized smart production and DSCs during the early part of the coronavirus disease 2019 (COVID-19) pandemic, which significantly disrupted traditional supply chains, especially for high-demand medical and health products, including personal protective equipment such as facemasks and testing kits.[10] However, DSCs and smart manufacturing raise new concerns about IP security, as IP travelling along DSCs may be vulnerable to being hacked or misappropriated through the supply chain.[11] Also, digital files in the supply chain may also contain material that would infringe the IP of others. Commentators have been raising concerns about IP security in digital manufacturing, especially 3DP, as part of broader concerns about new manufacturing technologies, such as 3DP's disruptive effect on the theoretical underpinnings and effective enforcement of IP.[12] Again, the issue of IP security and countervailing interests, including access to knowledge and medical treatment, emerged during the COVID-19 pandemic, where a particularly prominent case involved two engineers in Italy making replacement parts for a patented ventilator machine used to treat COVID patients threatened with litigation for allegedly infringing the patent.[13] While in the end the case never

1 See eg Matthew Sag, 'Internet Safe Harbors and the Transformation of Copyright Law' (2017) 93 *Notre Dame Law Review* 499; Maurizio Borghi, 'Chasing Copyright Infringement in the Streaming Landscape' (2011) 42 *International Review of Intellectual Property and Competition Law* 316.

2 See eg Amanda Scardamaglia and Angela Daly, 'Google, Online Search and Consumer Confusion in Australia' (2016) 24 *International Journal of Law and Information Technology* 203; Colleen V Chien, 'Of Trolls, Davids, Goliaths and Kings: Narratives and Evidence in the Litigation of High-Tech Patents' (2009) 87 *North Carolina Law Review* 1571.

3 See eg Daniel Gervais, 'Exploring the Interfaces between Big Data and Intellectual Property Law' (2019) 10 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 3.

4 Belinda Bennett and Angela Daly, 'Recognising Rights for Robots: Can We? Will We? Should We?' (2020) 12 *Law, Innovation and Technology* 60; Angela Daly, *Socio-Legal Aspects of the 3D Printing Revolution* (Palgrave Macmillan 2016); Björn Lundqvist, 'Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet-of-Things World: The Issue of Accessing Data' in Mor Bakhoum and others (eds) *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Springer Berlin Heidelberg 2018).

5 Jarkko Moilanen and others, 'Cultures of Sharing in 3D Printing: What Can We Learn from the Licence Choices of Thingiverse Users?' (2015) *Journal of Peer Production*. 6: pp 1–9.

6 Miia Martinsuo and Toni Luomaranta, 'Adopting Additive Manufacturing in SMEs: Exploring the Challenges and Solutions' (2018) 29 *Journal of Manufacturing Technology Management* 937.

7 Mojtaba Khorram Niaki and Fabio Nonino *The Management of Additive Manufacturing* (Springer International Publishing 2018).

8 Ling Jiang, 'Call for Copy—The Culture of Counterfeit in China' (2014) 2 *Journal of Chinese Economics* 73, However, it should be noted that China is transitioning from a user of IP (both legitimate and illegitimate) to a creator of its own IP. Kal Raustiala, 'Innovation in the Information Age: The United States, China, and the Struggle over Intellectual Property in the 21st Century' (2020) 58 *Columbia Journal of Transnational Law* 531.

9 Hing Kai Chan and others, 'The Impact of 3D Printing Technology on the Supply Chain: Manufacturing and Legal Perspectives' (2018) 205 *International Journal of Production Economics* 156.

10 Jane Feinmann, 'PPE: What Now for the Global Supply Chain?' (2020), pp 1–2 369 *BMJ*.

11 ibid.

12 Simon Bradshaw, Adrian Bowyer and Patrick Haufe, 'The Intellectual Property Implications of Low-Cost 3D Printing' (2010) 7 Scripted 6; Daly (n 4).

13 Jorge L Contreras, 'Research and Repair: Expanding Exceptions to Patent Infringement in Response to a Pandemic' (2020) 7 *Journal of Law and the Biosciences* 1.

reached a court, and the engineers may have been able to avail themselves of an exception to infringement, such threats may have a chilling effect on the use of distributed smart manufacturing.[14]

In this article, we focus on the issue of IP security in DSCs for smart manufacturing using 3DP or AM to consider (i) the extent to which IP is disrupted or weakened in DSCs and (ii) how IP is secured in these chains to mitigate such concerns. We summarize the relationship between 3DP and the law, focusing on IP, before considering how technical IP security measures have been mobilized in predecessor digital technologies. Here, we will focus on the debate around technological protection measures (TPMs) and digital rights management (DRM) as technical means of enforcing IP security. We consider how TPMs have been deployed in Internet-enabled content supply chains during the 1990s and 2000s, as well as the controversial legislative updates that accommodated DRM in that era, including the extent to which the right balance was struck between competing rights and interests. We then introduce more recent developments in IP security in DSCs before presenting our empirical research on this topic. Finally, we offer our concluding thoughts.

Three-Dimensional '3D' Printing and intellectual property law

ISO/ASTM 52900:2021[15] standard defines AM as follows:

> The process of joining materials to make parts from three-dimensional (3D) model data, usually layer upon layer, as opposed to subtractive manufacturing and formative manufacturing methodologies.

As visualized by Gibson et al,[16] 3DP or AM processes involve physical and digital processes or products used to produce a 3D physically manufactured output from a 3D digital model input. Since the second industrial revolution in the 1900s, assembly line manufacturing has shifted the overall manufacturing approaches towards distributed tasks in-house (assembly line) or outsourced (supply chain); therefore, different supply chain actors are involved in making a product.[17] In digital manufacturing, numerous supply chain actors are bound to generate, transmit and exchange digital data (which may contain sensitive or confidential information) as well as physical objects, both potentially containing IP. These processes differ from more traditional 'subtractive' manufacturing processes prevalent under the second industrial revolution, as the 3DP process involves creating a three-dimensional object from a digital design file and raw materials, which are placed in a layered fashion to create the final object (ie 'additive' manufacturing), rather than using a large block of raw material from which the desired object is 'subtracted'.[18] AM offers various advantages over traditional methods, including efficiency, precision, sustainability and the ability to produce objects or shapes that would be impossible according to traditional methods.[19]

AM is popularly known as 3DP (usually written as '3D printing'), including in the body of legal literature on the topic, so we adopt this term to describe the technology and manufacturing process. 3DP machines come in various sizes and at different price points, with the cheapest models (usually printing in plastics) retailing for under £100. More sophisticated machines that print other materials, such as metal and glass, can cost thousands or millions of pounds. However, open hardware projects like RepRap,[20,21] and no-cost design document repositories such as Thingiverse, along with low-cost 3DP machines, open up the 'democratizing' potential of 3DP compared to earlier manufacturing techniques.[22] In principle, anyone with a low-cost machine, access to low-cost plastic raw materials and an internet connection can start to produce objects that previously could only be manufactured on a mass, usually centralized, scale. This brings a number of efficiency and sustainability advantages. However, as may be evident by now, the diffusion of 3DP machines has not been as widespread as its potential might suggest: there may be other barriers to adoption, including the advantage that some technical knowledge would bring, the perceived or actual usefulness of and need for the machines and the often low-quality outputs of cheap 3DP machines compared to mass-produced consumer items readily and cheaply available in many retail stores.

14 Angela Daly 'Bioprinting Technology, Regulation, and Intellectual Property' in Deepak Kalaskar (ed) *3D Printing in Medicine* (2nd edn Woodhead Publishing 2022).

15 *ISO/ASTM 52900:2021—Additive Manufacturing—General Principles—Fundamentals and Vocabulary* (ISO/ASTM International 2021).

16 Ian Gibson and others, *Additive Manufacturing Technologies* (3rd edn, Springer International Publishing 2021) ch 1.

17 Mikell P Groover *Fundamentals of Modern Manufacturing* (7th edn, John Wiley & Sons, Inc 2020) ch 1.

18 K Satish Prakash, T Nancharaih and VV Subba Rao, 'Additive Manufacturing Techniques in Manufacturing -An Overview' (2018) 5 *Materials Today: Proceedings* 3873.

19 Gibson and others (n 16); Groover (n 17).

20 'RepRap' Available at https://www.reprap.org/wiki/RepRap (accessed 20 November 2022).

21 The RepRap project uses an open licencing approach on its website to freely share designs for parts of a 3D printing machine that can be assembled, using a few 'everyday' hardware items into a new functioning 3D printing machine.

22 Moilanen and others (n 5).

Various areas of law intersect with 3DP and DSCs.[23] Criminal or firearms legislation and IP are notable among these areas of law. The former has been thrust into the limelight due to the creation of firearms using 3DP machines, with the USA-based Defense Distributed's Liberator providing a very prominent and controversial example involving the company's distribution of design files that could be used with a 3DP machine to create a functioning gun.[24] Defense Distributed's right to distribute these files in the unusual context of the USA's expansive First Amendment right to free speech and the Second Amendment right to bear arms has been the subject of much debate and litigation in the USA and presents some alarming possibilities (although rarely realized in practice) for most other national jurisdictions in the world, which have more restrictive firearms laws than the USA.[25]

IP has also featured prominently in discussions over 3DP, but, to our knowledge, there has been no significant litigation in this domain. However, various pre-litigation disputes have taken place, mainly involving design files on intermediary platforms such as Thingiverse, and the utilization of notice and takedown schemes to remove, sometimes illegitimately, this content for alleged IP infringement.[26] Another example of this phenomenon is the recent threat of litigation vis-à-vis the Italian engineers' 3DP replacement valve parts during the COVID-19 pandemic, as mentioned earlier.[27] IP issues in 3DP mirror earlier concerns raised with the advent of the Internet: the digitalization of files potentially containing IP (especially copyright), the use of file-sharing sites and the emergence of new legal frameworks, such as the Digital Millennium Copyright Act in the USA and the European Union (EU)'s E-Commerce Directive, with their intermediary liability and notice and takedown schemes or provisions.[28]

However, 3DP differs from the previous digital content and Internet scenario. 3DP involves a more physical presence and production. This amplifies concerns about counterfeiting and 3DP, such as producing low-quality or unsafe products, and therefore brings in health, safety and consumer protection issues.[29] From an IP perspective, this means that copyright is no longer the focus area of IP law implicated by digital files: copyright concerns are accompanied by issues involving patents, trade marks and other IP rights, requiring a wider approach than the existing ones (eg there is no equivalent to the Digital Millennium Copyright Act in the USA for patents).[30]

There have been significant discussions on how 3DP and its DSCs pose risks to IP and how to address these risks.[31] Added complexities arise from the fact that IP rights are only harmonized to a certain extent at the international level through the World Intellectual Property Organization (WIPO) treaties and the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights; thus, there is still a significant divergence in how IP law operates in different national jurisdictions and how IP rights apply to cyber-physical manufacturing systems (also often called digital manufacturing systems).[32] This poses problems for supply chains, whether digital or traditional, since they are often transnational or global, transcending jurisdictional and national boundaries.

Furthermore, IP rights are not absolute rights: in certain situations, third parties can lawfully use IP without first seeking the rights holder or owner's permission. These exceptions, which differ for each IP right and between national jurisdictions, seek to ensure that the right balance is struck between different interest groups (especially IP owners and society at large) and that there is sufficient access to IP-protected materials for socially beneficial purposes. The precise balance to be struck between IP rights and exceptions is subject to fierce debate, as access to medicines such as human immunodeficiency viruses (HIV) or acquired immunodeficiency syndrome (AIDS) drugs and, more recently, access to COVID-19 vaccines and treatments demonstrate.[33] Accommodating these nuances of

23 Daly (n 4); Jasper L Tran, 'The Law and 3D Printing' (2015) 31 *The John Marshall Journal of Information Technology & Privacy Law* 505.

24 Angela Daly and others, '3D Printing, Policing and Crime' [2020] Policing and Society 1.

25 ibid.

26 Moilanen and others (n 5).

27 Daly (n 14); Dana Mahr and Sascha Dickel, 'Rethinking Intellectual Property Rights and Commons-Based Peer Production in Times of Crisis: The Case of COVID-19 and 3D Printed Medical Devices' (2020) 15 *Journal of Intellectual Property Law & Practice* 711.

28 Ben Depoorter, 'Intellectual Property Infringements & 3D Printing: Decentralized Piracy' (2014) 65 *Hastings Law Journal* 1483.

29 Daly (n 4); G Howells, 'Protecting Consumer Protection Values in the Fourth Industrial Revolution' (2020) 43 *Journal of Consumer Policy* 145; Geraldina Mattsson, 'Anti-Counterfeiting Concerns of the Vehicle Manufacturing Sector' (2015) 10 *Journal of Intellectual Property Law & Practice* 280.

30 Deven R Desai and Gerard N Magliocca, 'Patents, Meet Napster: 3D Printing and the Digitization of Things' (2014) 102 *The Georgetown Law Journal* 1691.

31 Daly (n 4); Rosa Maria Ballardini 'Intellectual Property Rights and Additive Manufacturing' in Eujin Pei, Mario Monzón and Alain Bernard (eds) *Additive Manufacturing—Developments in Training and Education* (Springer International Publishing 2019).

32 Daly (n 4); Adam Brown and others 'Legal Aspects of Protecting Intellectual Property in Additive Manufacturing' in Mason Rice and Sujeet Shenoi (eds) *Critical Infrastructure Protection X*, vol 485 (Springer International Publishing 2016).

33 Alexa B D'Angelo and others, 'Breaking Bad Patents: Learning from HIV/AIDS to Make COVID-19 Treatments Accessible' (2021) 16 *Global Public Health* 1523.

open-textured laws in digital systems that prefer more binary approaches ('can this design be lawfully used, or not?') is a challenge for IP law and DSCs[34] and one that may learn from the experience of TPMs.

Intellectual property, digital supply chains and technological protection measures

The risk of IP infringement is a prominent security priority within DSCs. Chhetri et al[35] have suggested that integrating emerging technologies of the fourth industrial revolution, including DSCs and 3DP, for product manufacturing and life cycle performance can pose various challenges to security requirements. Therefore, appropriately securing IP and data in DSCs remains a sophisticated and dynamic challenge.[36]

IP security is an ongoing challenge in law and practice for supply chains, predating their digitalization, but DSCs have introduced new security issues like increased frequency and impact from data breaches and cyberattacks.[37] Within DSCs, the flow of goods becomes dependent on credible information flows; therefore, it has become imperative to pay critical attention to the value embedded in the information exchanges.[38] A considerable amount of sensitive information, which may include IP and proprietary data, for making goods or delivering services is exchanged throughout DSCs, passing through decentralized digital and physical intermediaries for the product or its manufacturing information to reach the end user.[39] This can be contrasted with a traditional supply chain, where sensitive information is usually tightly controlled as it passes through centralized or semi-centralized intermediaries.[40] So, typically, a focal organization makes the product and retains the sensitive information such that the end user only receives the finished product in what is sometimes referred to as defensive silo gaps.[41] While, as mentioned earlier, traditional supply chains encounter IP risks, these risks may be increased in DSCs, making the IP security issue all the more relevant and dependent on the least secured player (ie the weakest link) within extended DSCs.[42]

There is limited evidence and research into IP infringements in DSCs, including quantitative research on the anticipated increased occurrence of IP infringement compared to traditional supply chains. As well as more theoretical legal literature on IP and 3DP expecting significant disruptions, including mass infringement,[43] Gartner predicted that 3DP use within DSCs would result in over US$100 billion annual revenue losses due to IP compromise at a global scale by 2018, on top of the already existing issues of IP infringements estimated to be worth over US$1 trillion.[44] Anusci[45] has questioned Gartner's claim for being difficult to measure or substantiate due to the elusive nature of IP within the digital space and the persistent issue of effectively measuring global IP infringement more generally. But at this point, 5 years after 2018, it appears that Gartner's claim has not come to pass. Indeed, there has been limited empirical evidence for the extent and scale of IP infringement in 3DP more generally. The limited literature that does exist affirms the theoretical challenge 3DP poses to conventional IP categories and enforcement; however, the widespread infringement is not occurring so far in practice.[46]

Various strategies and activities have been proposed to secure IP in DSCs, including the use of TPMs within the DSCs' communications flows and intermediary devices. Kerr et al define TPMs as follows:

> A technological method intended to promote the authorized use of digital works…accomplished by controlling access to

34 Emre Bayamlıoğlu and Ronald Leenes, 'The "Rule of Law" Implications of Data-Driven Decision-Making: A Techno-Regulatory Perspective' (2018) 10 *Law, Innovation and Technology* 295.

35 Sujit Rokka Chhetri and others, 'Manufacturing Supply Chain and Product Lifecycle Security in the Era of Industry 4.0' (2018) 2 *Journal of Hardware and Systems Security* 51.

36 Andrea M Matwyshyn, 'CYBER!' (2017) 2017 *BYU Law Review* 1109.

37 Igor Slabykh, 'The New Approaches to Digital Anti-Piracy in the Entertainment Industry' (2019) 19 *UIC Review of Intellectual Property Law* 75; Renee Wilson and Stephen J Shine, 'Is Your Data Protected? A Look at Cybersecurity Regulations in the US and EU' (2017) 10 *International In-House Counsel Journal* 1.

38 Amiya K Chakravarty, 'The Outsourcing Conundrum: Misappropriation of Intellectual Property in Supply Chains' (2021) 68 *Naval Research Logistics (NRL)* 229; Mohd Nishat Faisal, DK Banwet and Ravi Shankar, 'Information Risks Management in Supply Chains: An Assessment and Mitigation Framework' (2007) 20 *Journal of Enterprise Information Management* 677.

39 Pete Cooper, 'Aviation Cybersecurity' (2017).

40 Xiuhui Li and Qinan Wang, 'Coordination Mechanisms of Supply Chain Systems' (2007) 179 *European Journal of Operational Research* 1.

41 Nilufer Tuptuk and Stephen Hailes, 'Security of Smart Manufacturing Systems' (2018) 47 *Journal of Manufacturing Systems* 93.

42 Cooper (n 40).

43 Daly (n 4).

44 John Hornick, '3D Printing and IP Rights: The Elephant in the Room' (2015) 55 *Santa Clara Law Review* 801; Sharon Flank, 'Legal Issues in IP Protection for Additive Manufacturing' (2017) 4 *Texas A&M Journal of Property Law* 1.

45 Victor Anusci 'Gartner's Top 3 Failed Predictions on 3D Printing (That Will Probably Never Come True)' (2018). Available at https://www.3dprintingmedia.network/gartners-top-3-predictions-3d-printing-not-come-true-probably-never-will/ (accessed 19 April 2019).

46 Dinusha Mendis and Davide Secchi, 'A Legal and Empirical Study of 3D Printing Online Platforms and an Analysis of User Behaviour' (2015); Thomas Birtchnell and others, '3D Printing and Intellectual Property Futures' (2018).

such works or various uses of such works, including copying, distribution, performance, and display.[47]

TPMs used for 3DP applications within supply chains include using distributed ledger technology (eg blockchain) and DRM or chemical tagging to prevent counterfeiting, overrun production and facilitate distributed 'off-site or geo-market' manufacturing.[48] However, using technical solutions to protect IP in DSCs may impede lawful uses of such IP consistent with exceptions to infringement. Matwyshyn[49] and Wheatley[50] have indicated that such overreach by TPMs in previous digital technologies, especially the Internet, is a recognized problem. One way of mitigating this overreach and facilitating permitted uses of IP-protected material is to circumvent the TPM using technical means, eg decrypting an encrypted TPM. This is usually done without the permission of the IP owner or the party that implemented the TPM. However, circumvention of a TPM can also allow the IP-protected material to be used for purposes that would infringe the IP. Therefore, circumventing TPMs is a 'dual use' method, which can be used for legitimate and illegitimate purposes.

The illegal circumvention of TPMs was recognized and legislated against in the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT).[51] Both contain a provision (WCT Article 11 and WPPT Article 18, respectively) that instructs Contracting Parties to 'provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures' used by authors and performers, in addition to the legal provisions protecting the underlying IP (in this case, copyright). It is important to note that these treaties and provisions addressed TPMs and copyright, whereas 3DP also brings into play other IP rights. The TPM provisions in the WCT and WPPT have often permitted rightsholders to control copyright works 'to a much greater degree' than national copyright laws in many jurisdictions have 'traditionally allowed'[52] and facilitate the overprotection of copyright-protected works by not adequately recognizing legitimate uses of those works (ie covered by an exception or defense to infringement). The WIPO TPM provisions have been implemented in many national jurisdictions, such as through Articles 6 and 7 of the EU's Infosoc Directive (and in turn, Section 296 of the UK's Copyright, Designs and Patents Act 1988) and Section 1201 of the USA's Digital Millennium Copyright Act 1998. Some jurisdictions recognize exceptions to the anti-circumvention measures, eg for implementing the WIPO Marrakesh Treaty to make works accessible to blind people (see, eg Section 296ZE of the UK's Copyright, Designs and Patents Act).[53] However, the procedures for using these exceptions are often awkward, time-consuming and cumbersome (eg the need for a potential copyright user to complain to the UK Secretary of State if unable to do a 'permitted act' because of a TPM). The US process, which involves the Copyright Office in the Library of Congress designating exceptions to TPM circumvention every 3 years, while in theory a 'powerful tool for representing the public interest', in practice 'has consistently prioritized the interests of copyright holders'.[54]

Thus, the issue of securing IP in DSCs while facilitating permitted uses under exceptions remains a challenge. Concerns have been raised recently about how TPMs may impede the repair of products, as repair is not currently recognized as a copyright exception in many jurisdictions,[55] and indeed, rightsholders have leveraged IP law (among other strategies) to stymie consumers repairing products with third-party spare parts, causing social, economic and environmental detriment.[56] More efficient repairs and the ability to print spare parts are

47 Ian R Kerr, Alana Maurushat and Christian S Tacit, 'Technical Protection Measures: Tilting at Copyright's Windmill' (2002) 34 *Ottawa Law Review* 7.

48 Martin Holland, Josip Stjepandić and Christopher Nigischer, 'Intellectual Property Protection of 3D Print Supply Chain with Blockchain Technology', *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)* (IEEE 2018); ZC Kennedy and others, 'Enhanced Anti-Counterfeiting Measures for Additive Manufacturing: Coupling Lanthanide Nanomaterial Chemical Signatures with Blockchain Technology' (2017) 5 *Journal of Materials Chemistry C* 9570; Sam Davies 'Moog's Connecting Flight to Distributed Manufacturing—TCT Magazine' (*TCT Magazine*, 2019). Available at https://www.tctmagazine.com/3d-printing-news/moogs-connecting-flight-to-distributed-manufacturing/?mc_cid=a4b99d53fd&mc_eid=f45e8f24ac (accessed 14 August 2019).

49 (n 34).

50 Christopher T Wheatley, 'Overreaching Technological Means for Protection of Copyright: Identifying the Limits of Copyright in Works in Digital Form in the United States and the United Kingdom' (2008) 7 *Washington University Global Studies Law Review* 353.

51 Kerr, Maurushat and Tacit (n 48).

52 Ian R Kerr, 'Technological Protection Measures: Part II – the Legal Protection of TPMs' (2004).

53 Shae Fitzpatrick, 'Setting Its Sights on the Marrakesh Treaty: The U.S. Role in Alleviating the Book Famine for Persons With Print Disabilities' (2014) 37 *Boston College International and Comparative Law Review* 139; Jade Kouletakis, 'No Man Is an Island: A Critical Analysis of the UK's Implementation of the Marrakesh Treaty' (2020) 17 *SCRIPT-ed* 54.

54 MC Forelle, 'Copyright and the Modern Car: Colliding Visions of the Public Good in DMCA Section 1201 Anti-Circumvention Proceedings' (2023) 25 *New Media & Society* 628.

55 Anthony D Rosborou, 'Unscrewing the Future: The Right to Repair and the Circumvention of Software TPMs in the EU' (2020) 11 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 26.

56 Aaron Perzanowski *The Right to Repair* (Cambridge University Press 2022).

vital activities which DSCs facilitate,[57] thus any limitation to these activities may negatively affect innovation and efficiency,[58] although this is still subject to debate.[59]

In addition to the risk of intermediaries or end users in the DSC infringing IP, the IP embedded within the DSC can result in the digital aspects of the manufacturing process (rather than the final physical artefacts or products) becoming highly valuable for targeted attacks.[60] As well as constituting IP infringement, such attacks may be considered cybercrimes and subject to cybercrime law and enforcement. DSC operators may, depending on the context and circumstances, have obligations to comply with cybersecurity requirements, such as the EU's NIS Directive for critical infrastructure (implemented and retained in the UK via the NIS Regulations 2018), and personal data protection requirements, such as the EU's General Data Protection Regulation (also retained for the time being in the UK).[61] This raises another set of issues and concerns about user privacy and the use of data in cyber-physical manufacturing systems.[62] As 3DP is highly dependent on digital or computing technologies, ongoing debates about whether evolved technological tools (in particular AI) capable of creating IP within DSCs deserve any form of IP protection are also relevant.[63] Yet there is still a lack of international consensus on legal standards and requirements in these areas, which adds more complexity to securing DSCs, especially cyber-physical manufacturing systems operating within such supply chains, from a legal perspective.

57 Marco Savastano and others '3-D Printing in the Spare Parts Supply Chain: An Explorative Study in the Automotive Industry' in Leonardo Caporarello and others (eds) *Digitally Supported Innovation* (Springer International Publishing 2016); Jing-Sheng Song and Yue Zhang, 'Stock or Print? Impact of 3-D Printing on Spare Parts Logistics' (2020) 66 *Management Science* 3860.

58 Michele Boldrin and David K Levine *Against Intellectual Monopoly* (Cambridge University Press 2008).

59 Stefan Bechtold, '3D Printing and the Intellectual Property System' (2015) 28.

60 Simon Goldenberg and others, '3D Opportunity and Cyber Risk Management: Additive Manufacturing Secures the Thread' (2016).

61 Sumit Kumar and Shashikala Tapaswi, 'A Centralized Detection and Prevention Technique against ARP Poisoning', *Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012* (2012); Lachlan Urquhart and Derek McAuley, 'Avoiding the Internet of Insecure Industrial Things' (2018) 34 *Computer Law and Security Review* 450; Tania Wallis and Chris Johnson, 'Implementing the NIS Directive, Driving Cybersecurity Improvements for Essential Services', *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (IEEE 2020).

62 Yosef Ashibani and Qusay H Mahmoud, 'Cyber Physical Systems Security: Analysis, Challenges and Solutions' (2017) 68 *Computers & Security* 81.

63 Russ Pearlman, 'Recognizing Artificial Intelligence (AI) as Authors and Investors under U.S. Intellectual Property Law' (2018) 24 *Richmond Journal of Law & Technology* i; Amir H Khoury, 'Intellectual Property Rights for "Hubots": On the Legal Implications of Human-like Robots as Innovators and Creators' (2017) 35 *Cardozo Arts & Entertainment Law Journal* 635.

Technological advancements in IP asset management may have facilitated the effective use of TPMs beyond conventional IP protection. For example, TPMs may be applied as early as the IP inception stage (start-of-life) and may extend to the IP retiring stage (end-of-life), in what we illustrate in Fig. 1 as a contributing factor for the increasing preference to secure IP with TPMs.

Nevertheless, it is also worth mentioning that the extended reach also introduces additional security issues and concerns across the DSC, including IP, which are worth exploring; however, this is beyond the scope of our research and, thus, an opportunity for further investigation.

In summary, securing IP in supply chains used to operate cyber-physical manufacturing systems presents various recognised issues in IP security, from divergence in legal regimes in different jurisdictions (despite some level of harmonization via WIPO treaties), to the potential for overreach in applying TPMs, to the use of concepts developed for copyright for other areas of IP (patents, design rights and trade marks). The limited empirical research on 3DP and IP to date has generally involved information neither about how vital IP security is for those using 3DP and DSCs nor about what strategies they employ to secure IP if necessary. We now turn to what happens in practice and present insights from our research to address this gap.

Intellectual property strategies for digital manufacturing supply chains

There is no unified or uniform definition of a DSC in the literature, and it is not a legal term. We define a DSC as follows, elaborating on the various definitions gathered by Büyüközkan and Göçer:

> An intelligent best-fit technological system that is based on the capability of massive data disposal and excellent cooperation and communication for digital hardware, software, and networks to support and synchronise interaction between organisations by making services more valuable, accessible, and affordable with consistent, agile, and effective outcomes.[64]

The focus of our discussion is based on the product- or service-based supply chain model, which is encapsulated by enhancements driven by the digital space and manifested in the physical space, as demonstrated by 3DP. We understand that both the actors and processes involved in the supply chain tap into the digital space to generate

64 Gülçin Büyüközkan and Fethullah Göçer, 'Digital Supply Chain: Literature Review and a Proposed Framework for Future Research' (2018) 97 *Computers in Industry* 157.

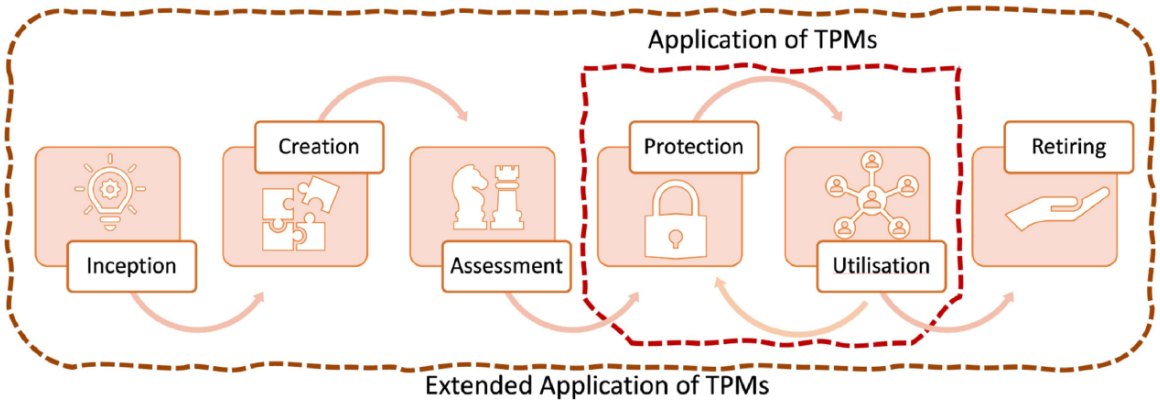

Figure 1. Intellectual property asset management and technological protection measure life cycle.

digitalised materials and objects that are associated with equivalents of outputs that exist in the physical space and can be triggered or activated from either the digital or physical space.[65] The supply chain we focus on is what we refer to as a DSC, a term commonly used in engineering. Büyüközkan and Göçer[66] suggest that digital transformation is not about making every process or item exist in the digital space (digitization); it concerns employing the existing and novel digital technologies to support the concepts of concurrent process and role executions within the supply chain. This allows us to investigate 3D printing as a cyber-physical system conduit within the smart manufacturing era for a holistic view of interactions and processes across the DSC.

Complexities of existing supply chains are an ongoing global challenge.[67] The global COVID-19 pandemic has evidenced this point: however, some organizations operating within DSCs have provided evidence of the enhanced synergy between DSCs and traditional supply chains.[68] Even where these synergies take place, DSCs also inherit or even intensify some of the challenges of both traditional supply chains and DSCs.[69] DSCs are not a magic formula that automatically reduces pre-existing risks and challenges, so one must consider consequences linked to their level or intensity of integration with digital tools and associated digital technologies.

65 Claudia Lizette Garay-Rondero and others, 'Digital Supply Chain Model in Industry 4.0' (2019) 31 *Journal of Manufacturing Technology Management* 887.

66 Büyüközkan and Göçer (n 64).

67 Seyda Serdarasan, 'A Review of Supply Chain Complexity Drivers' (2013) 66 *Computers & Industrial Engineering* 533.

68 Abirami Raja Santhi and Padmakumar Muthuswamy, 'Pandemic, War, Natural Calamities, and Sustainability: Industry 4.0 Technologies to Overcome Traditional and Contemporary Supply Chain Challenges' (2022) 6 *Logistics* 81.

69 Ling Xue and others, 'Risk Mitigation in Supply Chain Digitization: System Modularity and Information Technology Governance' (2013) 30 *Journal of Management Information Systems* 325.

Two key risks of digitalizing the supply chain are (i) losing control over manufacturing data previously held in-house and (ii) experiencing service disruptions due to digital support services not being available on demand.[70] These events may comprise materials protected by IP rights and confidentiality (eg trade secrets). Thus, also in light of the increased frequency of cyber-attacks in the manufacturing sector, researchers, practitioners and customers have called for DSC operators to secure the supply chain and monitor the compliance of suppliers.[71] However, there has been limited research on how these challenges are addressed in practice in 3DP DSCs, especially from the perspective of IP security. To understand this issue better, we present some results from empirical research that we have conducted on stakeholder views and practices.[72]

Methodology and limitations

We developed an online self-administered questionnaire (SAQ) using the Qualtrics platform, which was distributed to participants who had experience with IP security issues in 3DP/AM DSCs, to obtain their responses about securing the IP of AM applications within supply chains from March 2021 to June 2022.[73] Qualtrics was chosen because it is flexible to adaptations, helps distribute access to participants, organizes the data collection process and supports result reporting or exporting to other formats in a manner accessible to the researchers'

70 Garay-Rondero and others (n 65).

71 Make UK, 'Cyber Security and Manufacturing: A Briefing for Manufacturers' (2019).

72 This research is part of the lead author's PhD research project, supervised by a team including the second author.

73 Data used in this paper were acquired via an online self-administered survey conducted from March 2021 to June 2022.

analysis software.[74] This online questionnaire instrument was considered apt for surveying the descriptive nature and emerging relationships between the key aspects of our subject matter.[75] We used the term 'additive manufacturing' in the survey rather than '3D printing', as it is more widely used in expert circles.

The survey asked participants a series of questions to measure and describe their views and experience with IP issues when AM is used as the primary manufacturing process within a DSC. The two key questions were as follows:

- Have you had any challenges securing and managing your IP when using AM in the supply chain?
- Have you had any potential challenges with determining appropriate IP securities for using AM within the supply chain?

We also asked additional questions, which helped provide some background on the topic and highlight the perceptions of participants. For example:

- Do you consider IP an enabler or a barrier to using AM within supply chains?
- Do you consider securing the IP of AM a barrier or an enabler to using AM within supply chains?

Finally, the participants were asked about the strategies they would choose to secure their IP within a DSC context when primarily using AM:

- Please indicate what combinations of strategies for securing and managing IP you shall opt for when using AM in a supply chain.

The responses were analysed statistically with the aid of MS Excel to obtain the descriptive overview (descriptive statistics and correlation) of respondents at the aggregated group and categorical subgroup levels. This enabled us to identify potential trends on the degree of intellectual risk encounters, perspectives about IP effects and preference for IP security strategies.[76] Finally, the findings were reflected upon, with literature on IP, AM and TPMs applied to this area. Such empirical research methods are deemed applicable across multiple disciplines, including law and engineering management, thus reaffirming our chosen approach to address the issue.[77]

We sought people with prior expertise in some aspects of 3DP, DSCs and IP to participate in the online questionnaires. This purposive sampling necessarily involved a limitation of our, to some degree subjective, judgment about whom we considered as suitable candidates to participate in the research. We recruited participants via peer referrals from previous participants (ie using the snowballing method), online profile browsing on professional and social networks (eg LinkedIn and ResearchGate) and contacting institutions considered to be operating in the fields of interest.[78]

A major limitation of our sampling technique was a potential bias in participant selection (eg incorrect or missing information in social network profiles may have resulted in inappropriate inclusion or exclusion) although pre-survey discussions were held to determine whether participants possessed relevant subject-matter knowledge and expertise. Furthermore, surveys conducted using online SAQs are usually identified as having a broad outreach, yet they have a lower progression and completion rate.[79] Indeed, the time required for completion of the survey was expected to be a significant issue: to limit the issue, we have issued each participant with a unique link that enabled them to return and resume work wherever they decided to pause it. Additionally, periodic prompts were given to participants to encourage their progression to completion.

Findings: *participant demographics*

Thirty-seven participants from North America, Europe, Africa and Asia-Pacific responded to our questions. They came from various backgrounds, which we have grouped under the following headings: Academic, Legal, Managerial and Engineering. As illustrated in Fig. 2, most of our respondents' backgrounds were in managerial or engineering roles, followed by a handful in academic roles; the least represented were those in legal roles. Many of our participants had senior-level positions, eg senior managers, senior engineers and senior academics (professors).

This revealed a distribution of expertise across the fields of AM, IP, supply chain, cyber-physical security and

74 Jessica T DeCuir-Gunby and Paul A Schutz *Developing a Mixed Methods Proposal: A Practical Guide for Beginning Researchers* (SAGE Publications, Inc 2017).

75 John W Creswell and J David Creswell *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th edn SAGE Publications Inc 2018).

76 Lior Gideon (ed) *Handbook of Survey Methodology for the Social Sciences* (Springer New York 2012).

77 Dawn Watkins and Mandy Burton (eds) *Research Methods in Law* (2nd edn Routledge 2018); Mark NK Saunders, Philip Lewis and Adrian Thornhill *Research Methods for Business Students* (8th edn Pearson Education 2019).

78 Kenneth S Bordens and Bruce B Abbott *Research Design and Methods: A Process Approach* (10th edn McGraw-Hill Education 2018).

79 Alan Bryman and Edward Bell *Social Research Methods* (5th edn Oxford University Press Canada 2019).

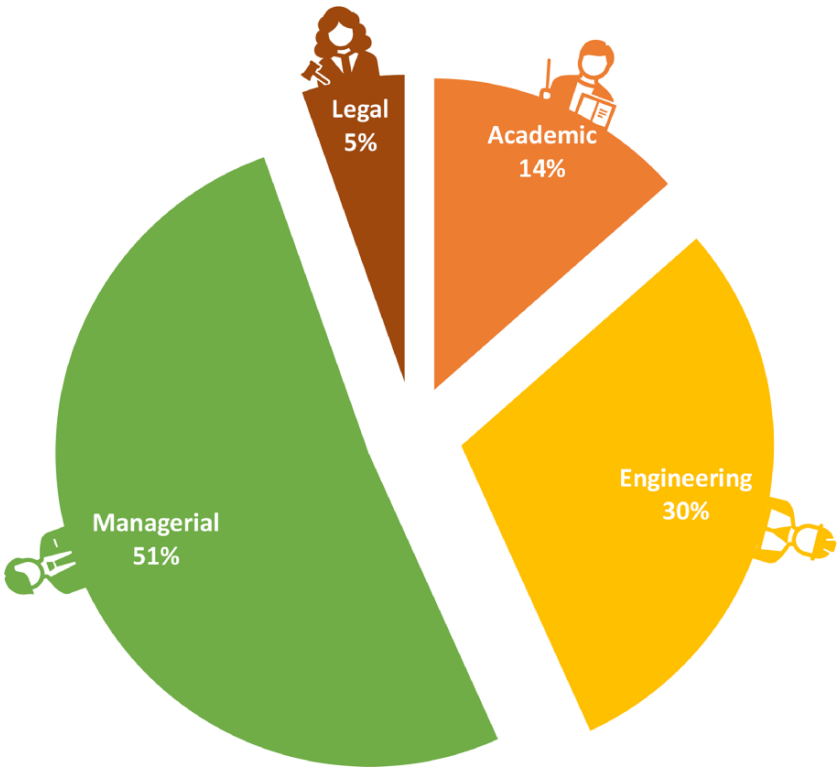

Figure 2. Participant expertise or role demographics.

strategic management from technical and non-technical backgrounds.

Findings: *experience with intellectual property in additive manufacturing supply chains*

The participants were asked about their experience of challenges in securing IP and determining IP security for AM applications within supply chains in two separate questions. Fig. 3 reveals that the participants had mostly encountered no challenges securing IP and determining an IP security strategy for AM use within the supply chain. Nevertheless, some participants declared that they had or may have had such challenging encounters when using AM within supply chains. We use the term 'Additive Manufacturing Supply Chains' as an abridged expression in headings and captions to refer to supply chains that use AM as their primary method of producing or servicing objects/parts.

It was further observed that, despite fewer participants answering 'yes' (13 per cent) and 'maybe' (22 per cent) to whether they had encountered challenges with securing IP, the ordering reversed with relatively more participants indicating 'yes' (24 per cent) and 'maybe' (19 per cent) to whether they encountered challenges in determining an IP strategy for AM use within supply chains.

Findings: *effects of intellectual property on additive manufacturing supply chain*

In two questions, participants were then asked about their perceptions of the effect of IP and its security on using AM within supply chains. One question asked whether IP was a barrier or an enabler to using AM within supply chains, and another asked whether securing IP was a barrier or an enabler to using AM within supply chains. Fig. 4 shows that participants were mainly of the view that IP, as well as securing IP, is both a barrier and an enabler to using AM within the supply chain.

It is further observed that for both questions on IP and securing IP, the participants' views were significantly similar about whether it was a barrier (19 per cent of respondents) or an enabler (16 per cent of respondents). Nevertheless, when the responses of barrier or enabler are combined, they account for about a third of respondents; this is closer to the results of participants who see the effect as both a barrier and an enabler (46 per cent and 43 per cent). Nevertheless, about a fifth of participants

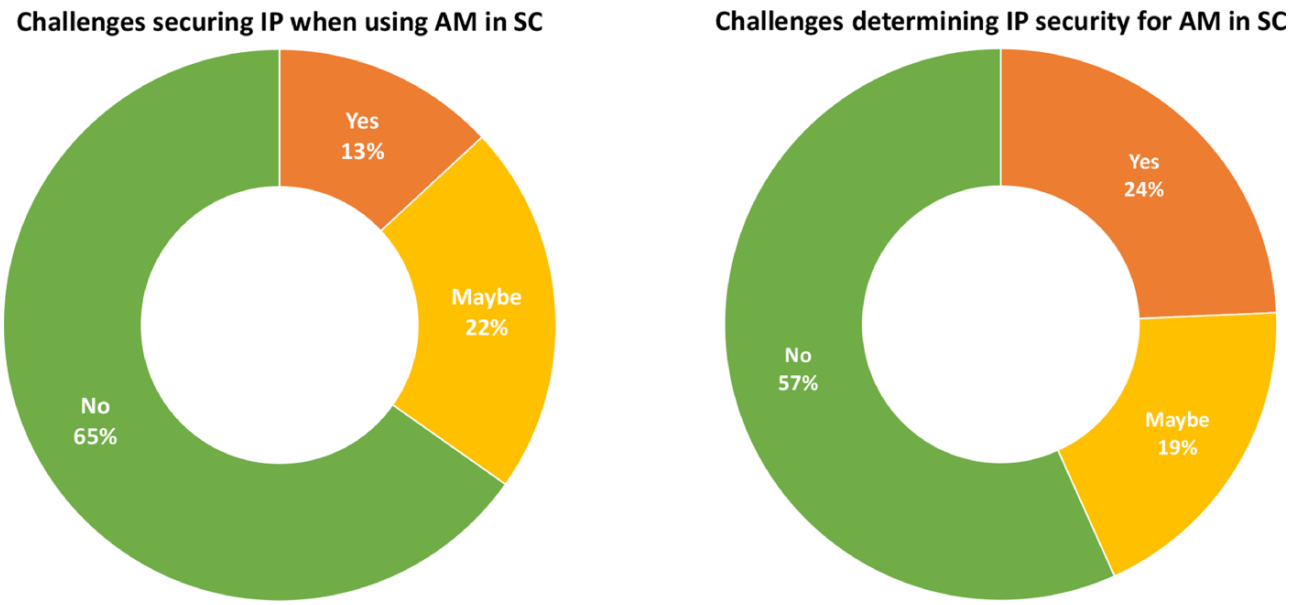

Figure 3. Encounters with intellectual property on additive manufacturing supply chains.

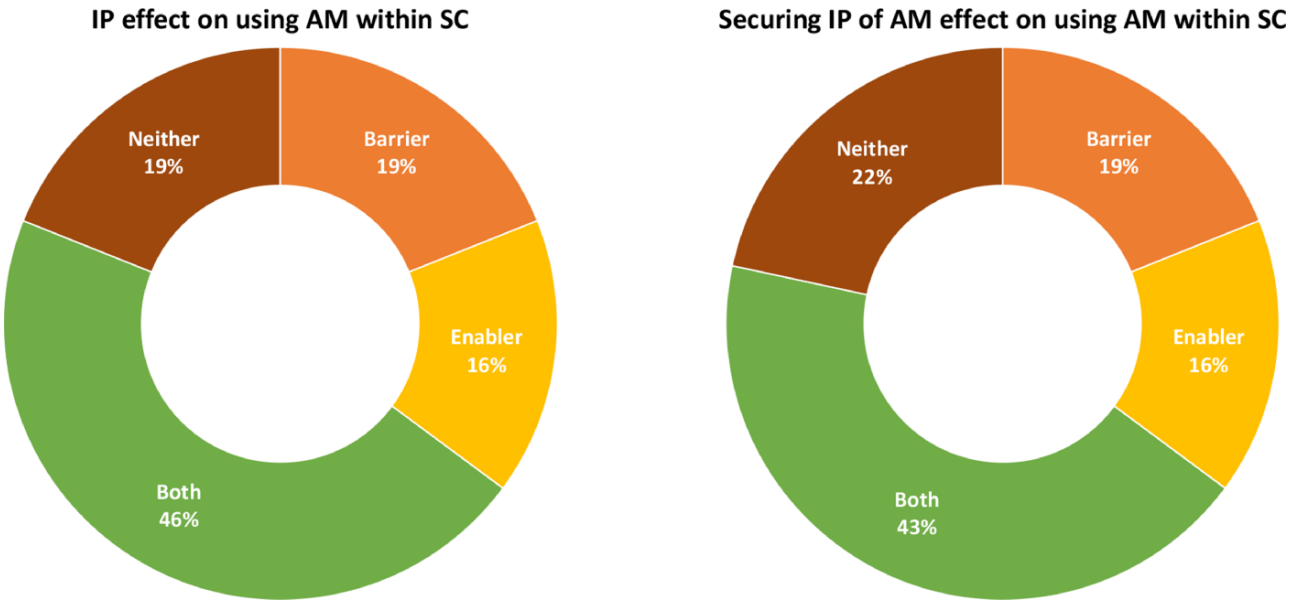

Figure 4. Perceived effects of intellectual property on additive manufacturing supply chains.

believe that these are neither a barrier nor an enabler (19 per cent and 22 per cent).

Findings: *intellectual property security strategies for additive manufacturing supply chains*

We then asked participants about their IP security and management strategies for AM use in the supply chain. Unlike the previous questions, participants could select multiple options for this answer. Fig. 5 illustrates that participants strongly preferred using technical approaches (eg TPMs) to manage and secure IP when using AM in a supply chain. This was followed by secrecy approaches (ie confidentiality), with legal approaches (eg registered protection in IP law such as a patent) coming third. A handful of participants indicated that an unrestrictive approach (ie open access licensing) was suitable, and the least popular option was 'disregard' (ie not adopting any IP security measures).

Each approach was chosen, at least once, by different participants; however, the participants' choices comprised various combinations (as they could select more

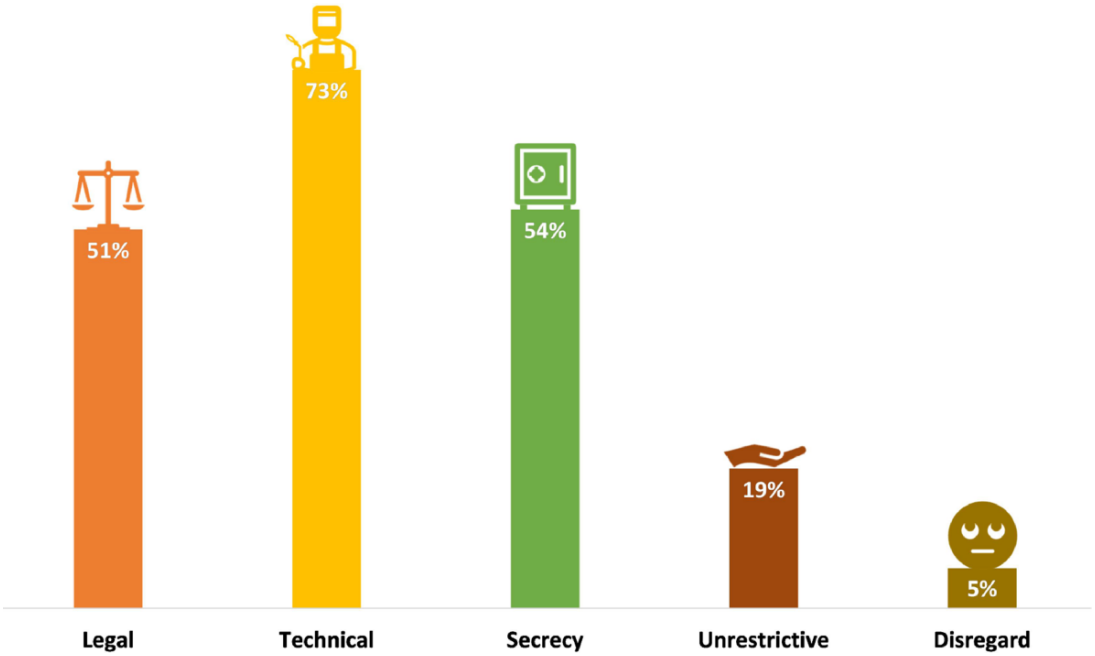

Figure 5. Intellectual property security strategy preference.

than one strategy), producing 12 different patterns. The technical approach was included in eight combinations (67 per cent of patterns), followed by the legal approach and the secrecy approach each contained in seven combinations (58 per cent of patterns). Interestingly, the unrestrictive approach accounted for four combinations (33 per cent of patterns), while the disregard approach emerged in two combinations (17 per cent of patterns) as the least popular IP strategy.

The most popular IP strategy mix comprised legal and technical combined (selected by 22 per cent of respondents). This was followed by (i) legal, technical and secrecy combined (selected by 16 per cent of respondents); (ii) technical and secrecy combined, as well as secrecy alone (selected by 14 per cent of respondents each); (iii) technical and unrestrictive combined (selected by 8 per cent of respondents) and (iv) unrestrictive alone and technical alone (selected by 5 per cent of respondents each). Among the least popular IP strategies (each selected by 3 per cent of respondents), we observed a combination of four approaches—legal, technical, secrecy and disregard; as well as legal, technical, secrecy and unrestrictive; then a combination of three approaches—legal, technical and unrestrictive; as well as legal, secrecy and disregard; finally, a combination of legal and secrecy. No participants selected the legal approach as the sole means to address IP security issues.

Findings: *intellectual property security strategies and perceived effect relationships*

A correlational analysis was conducted on the participants' responses to identify relationships within the previous results. This enabled us to examine emerging trends that related the perceived effects of IP on AM use within supply chains (Fig. 4) to the types of IP security strategies that are considered (Fig. 5). Fig. 6 presents the merged results and relationships.

We observed that all the IP security and management approaches were considered worthwhile deploying for questions about the effect of IP on using AM within the supply chain, in which participants indicated that they perceived it as both a barrier and an enabler. As such, the participants' favoured strategies were again a technical approach (30 per cent), a secrecy approach (22 per cent), a legal approach (19 per cent), an unrestrictive approach (11 per cent) and a disregard approach (5 per cent) in descending order. Similarly, participants indicated that their preferred strategies for securing IP's effect on using AM within the supply chain were in favour of a technical approach (38 per cent), a legal approach (22 per cent), a secrecy approach (19 per cent), an unrestrictive approach (11 per cent) and a disregard approach (3 per cent) in descending order.

Participants who indicated that they consider IP's effect on using AM within the supply chains as

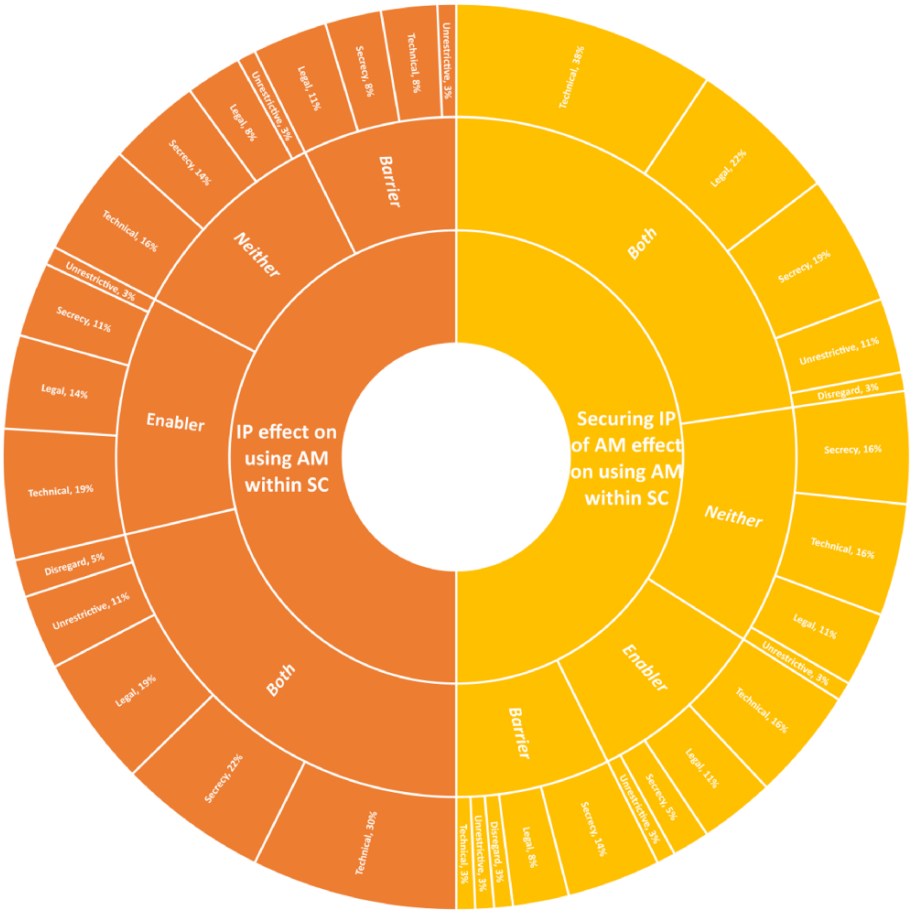

Figure 6. Intellectual property security strategy and perceived effects on additive manufacturing supply chains.

neither a barrier nor an enabler also favoured a technical approach (16 per cent), a secrecy approach (14 per cent each), a legal approach (8 per cent) and an unrestrictive approach (3 per cent) in descending order, as strategies for securing IP. Meanwhile, participants who indicated that they consider securing IP's effect on using AM within the supply chains as neither a barrier nor an enabler preferred technical and secrecy approaches (16 per cent each) over a legal approach (11 per cent) and an unrestrictive approach (3 per cent).

Interestingly, when participants considered that IP's effect on using AM within the supply chains was a barrier, the strategy that was mainly associated with that condition was a legal approach (11 per cent), followed equally by secrecy and technical approaches (8 per cent each) and, finally, an unrestrictive approach (3 per cent). Nevertheless, when securing IP's effect on using AM within the supply chains was considered as a barrier, the preferred strategy that emerged was equally dominantly in favour of a secrecy approach (14 per cent), followed by considerations for a legal approach (8 per cent), then equally followed by disregard, unrestrictive and technical approaches (3 per cent each).

Finally, when IP's effect on using AM within the supply chains was considered as an enabler, participants indicated their preference for a technical approach (19 per cent) over a legal approach (14 per cent), followed by a secrecy approach (11 per cent), then finally an unrestrictive approach (3 per cent) as strategies for securing IP on using AM within the supply chains in descending order. However, when securing IP's effect on using AM within the supply chains was considered as an enabler, participants indicated a preference for a technical approach (16 per cent), a legal approach (11 per cent), a secrecy approach (5 per cent) and an unrestrictive approach (3 per cent) in descending order.

The results revealed that TPMs (technical approach), despite their shortcomings, are the preferred strategy to secure intellectual creations and innovations in the context of AM applications within supply chains. Secrecy is another strategy especially favoured when securing IP poses a barrier to using AM within the supply chains.

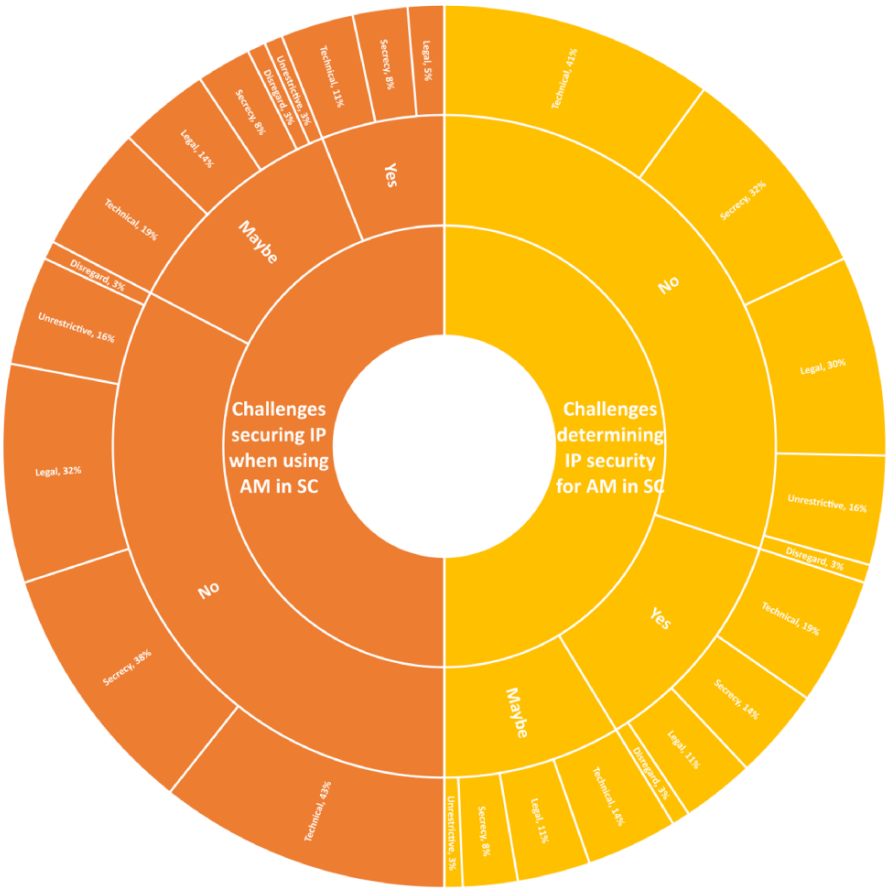

Figure 7. Intellectual property security strategy and encounters with intellectual property challenges.

Findings: *intellectual property security strategies and encountered challenges relationships*

Another correlational analysis was conducted on participants' responses to determine relationships within the previous results. This enabled us to examine emerging trends that related the declared IP challenges encountered when using AM within supply chains (Fig. 3) to the types of IP security strategies that participants prefer (Fig. 5). Fig. 7 presents the merged results and relationships.

Despite many participants indicating that they have faced no challenges in securing IP or determining IP security strategies, their answers showed that they explored all strategy options to secure their IP when using AM within supply chains. More specifically, these respondents indicated that their preferences were in favour of a technical approach (43 per cent) and a secrecy approach (38 per cent) over a legal approach (32 per cent), an unrestrictive approach (16 per cent) and a disregard approach (3 per cent) when faced with the challenge of securing IP when using AM within supply chains. Similarly, the results revealed that these respondents further indicated their preference mainly for a technical approach (41 per cent), followed by a secrecy approach (32 per cent), a legal approach (30 per cent), an unrestrictive approach (16 per cent) and a disregard approach (3 per cent) when faced with the challenge of determining IP security strategies when using AM within supply chains.

Participants who answered 'maybe' to being exposed to IP challenges favoured the technical approach (19 per cent) and legal approach (14 per cent) over the secrecy (8 per cent), disregard and unrestrictive approaches (3 per cent each). For participants who answered 'maybe' to being challenged with determining IP security strategies when using AM within supply chains, only the top four popular IP security strategies were considered, namely technical approach (14 per cent), legal approach (11 per cent), secrecy approaches (8 per cent) and unrestrictive approach (3 per cent).

Finally, participants who indicated 'yes' to being challenged with securing IP when using AM within supply chains revealed a preference for a technical approach

(11 per cent) and a secrecy approach (8 per cent) over a legal approach (5 per cent); meanwhile, participants who indicated 'yes' to being challenged with determining IP security when using AM within supply chains had their strategies' preference in favour of a technical approach (19 per cent) and then a secrecy approach (14 per cent) before considering a legal approach (11 per cent) over a disregard approach (3 per cent).

It must be noted here that the top three IP security strategies (Fig. 4) were considered in all encounters with IP challenges when using AM within supply chains; however, the technical approach was the most dominant, followed by the secrecy approach, favoured over the legal approach.

Conclusion

Our results show the complexities of IP and IP security for digital manufacturing in DSCs, specifically 3DP or AM applications within such chains.

We discovered that most surveyed participants deemed IP to serve a dual purpose (ie both a barrier and an enabler to using 3DP/AM in DSC); similarly, most participants indicated that securing IP was considered both a barrier and an enabler to using 3DP/AM in DSCs. These responses may arise out of the participants' beneficial encounters with creating and using their own IP for 3DP/AM applications within DSCs (an enabler) and, on the other hand, their need to use others' IP (a barrier). However, the fact that this was the majority perspective suggests that views of IP being detrimental to 3DP/AM's operations within DSCs, or 3DP/AM disrupting traditional IP, are not prominent in practice (Fig. 3). Understanding this complexity in the role of IP and IP security is a topic for further, more in-depth research with expert stakeholders. Nevertheless, the participants employ several strategies to secure IP in those DSCs (Fig. 4), including formal legal protections (eg patent or design rights registration) that emerged as only the third most popularly preferred strategy. Instead, technical approaches to protect IP, using TPMs, are the most popularly preferred strategy for 3DP/AM use within DSCs, even if most participants would use these in combination with other strategies, including commercial confidentiality (secrecy) and registered protection (legal).

A further examination of subgroups formed from the participants' roles (Academic, Engineering, Legal and Managerial) based on cross-correlated response patterns (Figs. 5 and 6) revealed unique perspectives that could be associated with their degree of direct exposure to IP issues within DSCs that primarily use 3DP/AM.

Regarding 'IP security strategy and encounters with IP challenges', it was observed that amongst participants who encountered challenges with securing IP or challenges with determining appropriate IP security strategies (yes or maybe), a technical approach was the most preferred by both managerial and engineering roles; but academic roles preferred a secrecy approach; finally, legal roles were evenly inclined towards technical, secrecy and legal approaches when challenged with securing IP, yet no legal roles declared encountering a challenge determining an IP security strategy. This reinforces a preference pattern for TPMs across most roles. Still, it is worth noting that each role indicated more than one strategy preference; we infer from the legal roles' response patterns that they employed a pragmatic approach of exploring multiple options, and perhaps they aimed to strike some strategic balance to minimize IP (over)protection when using 3DP/AM within DSCs.

Regarding 'IP security strategy and perceived effects on AM supply chains', it was additionally observed that amongst participants who perceived a binary effect of IP or a binary effect of securing IP (barrier or enabler), technical and secrecy approaches were the most preferred by managerial roles; engineering roles mostly preferred a combination of legal, technical and secrecy approaches. Meanwhile, academic roles preferred a combination of legal, technical and unrestrictive approaches; finally, legal roles were similarly evenly inclined towards technical and legal approaches when perceiving the effect of IP, yet no legal roles declared a perceived binary effect when securing IP. Furthermore, amongst participants who perceived a dual effect of IP or a dual effect of securing IP (both a barrier and an enabler), managerial roles were mainly inclined towards a technical approach this time around, whilst engineering roles were inclined towards secrecy and technical approaches. Interestingly academic roles revealed a preference for all approaches (secrecy, unrestrictive, technical, legal and disregard), whilst legal roles were inclined towards technical, legal and secrecy approaches. The complexity faced on the ground by participants when handling IP was evident from the multiple approaches they preferred, but what was most interesting was the viewpoint of academic roles that may depict the critical views on IP being pluralistic in nature, especially when using 3DP/AM within DSCs. This may also reflect cultural norms within academia as regards a less commercially driven approach towards innovation and more positive attitudes towards open use

and dissemination of IP compared to other participant categories.[80]

One limitation of our research is that surveys are usually close-ended in their enquiry nature; so, since we did not conduct follow-up interviews with participants, we could not discover more about their decision-making on implementing these different strategies, in differing ways, in different circumstances or at different points in the DSCs, which are thus all topics for further research. Furthermore, our focus on 3DP/AM within DSCs may make it difficult to generalize our findings for all digital manufacturing supply chains and all IP jurisdictions; however, our work provides some relevant insights into the preferences that come into play and may be extended with further research to investigate the nature of responses in particular jurisdictions and digital manufacturing supply chains.

The participants' preference for using TPMs to secure IP for 3DP/AM applications within DSCs may be an efficient means of protecting and securing their own IP; however, it raises issues about the overreach of IP protection and the potentially detrimental effect on the legitimate uses of IP-protected materials by 3DP/AM users in DSC. This may inhibit some social and environmental benefits of using decentralized 3DP/AM, including printing spare parts, and may negatively affect further innovation related to 3DP/AM use within DSCs. Ensuring that legitimate IP protection is offered without an overreach into users' rights may be a topic for further research in 3DP/AM and DSCs, especially in the current context of disruption to conventional supply chains and the move to onshoring production and increasing sustainability in light of climate change challenges.

80 See eg Joshua M Pearce, Alexis S Pascaris and Chelsea Schelly, 'Professors Want to Share: Preliminary Survey Results on Establishing Open-Source-Endowed Professorships' (2022) 2 *SN Social Sciences* 203; Markus Perkmann and others, 'Academic Engagement and Commercialisation: A Review of the Literature on University–Industry Relations' (2013) 42 *Research Policy* 423.