

## Intellectual Property Management Challenges of Additive Manufacturing in Replacement Part Supply Chains

Kwaku Adu-Amankwa<sup>1</sup>, Jonathan Corney<sup>2</sup>, Athanasios Rentizelas<sup>3</sup>, Andrew Wodehouse<sup>4</sup>

<sup>1</sup>*Department of Design, Manufacturing and Engineering Management, University of Strathclyde, United Kingdom (Tel: 0141 548 2091; e-mail: [kwaku.adu-amankwa@strath.ac.uk](mailto:kwaku.adu-amankwa@strath.ac.uk))*

<sup>2</sup>*School of Engineering, University of Edinburgh, United Kingdom (e-mail: [j.r.corney@ed.ac.uk](mailto:j.r.corney@ed.ac.uk))*

<sup>3</sup>*School of Mechanical Engineering, National Technical University of Athens, Greece (e-mail: [arent@mail.ntua.gr](mailto:arent@mail.ntua.gr))*

<sup>4</sup>*Department of Design, Manufacturing and Engineering Management, University of Strathclyde, United Kingdom (e-mail: [andrew.wodehouse@strath.ac.uk](mailto:andrew.wodehouse@strath.ac.uk))*

**Abstract:** Additive manufacturing underpins Industry 4.0 and is often identified as having potential applications in replacement part supply chains; however, it also introduces complex challenges for existing governance structures, especially those linked to intellectual property security concerns. This paper quantitatively surveyed views of experts in management, engineering, and academic roles about their concerns regarding intellectual property security of additive manufacturing applications in replacement part supply chains. The findings reveal that despite the often-cited benefits there remain significant concerns about this technology's application from management and security perspectives within the Industry 4.0 era.

Copyright © 2022 The Authors. This is an open access article under the CC BY-NC-ND license (<https://creativecommons.org/licenses/by-nc-nd/4.0/>)

**Keywords:** Additive Manufacturing, Supply Chain Management, Intellectual Property, Replacement Parts, Concern Levels

### 1. INTRODUCTION

Industry 4.0 (I4.0) promises a digitally transformed state that productively integrates advanced and emerging technologies by building upon humans-machine collaboration and productive data sharing (Chhetri *et al.* 2018). Additive Manufacturing (AM) comprises several layer-wise fabrication technologies driven by digital model data; under I4.0, AM is gaining attention at personal, industry, business, and government levels due to persistent annual growth of the AM Industry's value (from \$4.1bn to \$11.9bn over 2015-2021), causing many to predict unprecedented disruptions to society (Wohlers Associates 2021). This progression has evolved AM's capabilities from being limited to the production of prototypes into the manufacture of final products such as a Replacement Part (RePt); thus, empowering AM to extend its original intents into innovate applications within various Supply Chain (SC) based on distinctively favourable features (Santoso and Wicker 2016, Birtchnell *et al.* 2018).

Intellectual Property (IP) appreciates creative intellects of individuals and though considered intangible; its significance has grown with a paradigm shift in favour of intangible assets over tangible assets from 17% to 84% over 1975-2015 (Ocean Tomo 2017). Nevertheless, there have been ongoing concerns about the impact of AM on existing IP and SC structures, due to AM's ability to elude IP constraints built into conventional manufacturing methods and the possibility of uncontrollable digitally distribution (Petrick and Simpson 2013, Hornick 2015). Gartner's prediction for over \$100bn losses from AM

use in SCs due to IP compromise by 2018, gave credibility to this concern (Hornick 2015, Anusci 2018). Although this prediction has not yet materialised; there is no consensus in the literature on whether this scale of disruption is likely to happen eventually. Consequently, authoritative bodies have been encouraged to monitor AM and its IP implications (Mendis *et al.* 2020). Such concerns demonstrate a persistent uncertainty about appropriate reactions towards this digitally disruptive technology's future impact on existing manufacturing structures (UK Additive Manufacturing Steering Group 2017). Moreover, IP of RePts is a grey area of discussion when AM is used due to conflicts from IP objectives, market competitions, and repair doctrines, especially regarding design rights associated with single-product RePt or RePt for a larger patent-protected assembly (European Commission 2004, Götting and Hetmank 2019). Essentially, RePts from AM embody a complex mix of digital and physical IP, whereas traditionally manufactured RePt contain solely relatively simplified physical IP (Weinberg 2016).

A Replacement-Part Supply Chain (*RePtSC*) comprise a network of people, equipment and technologies using information and resource (*material, intellect, and finance*) within organisations to perform tasks that are required to sustain overall customer utility, satisfaction, and loyalty (Driessen *et al.* 2014, Mcdermott *et al.* 2021). RePtSCs are established in pre-delivery stages (primary market) and operated in the post-delivery stages (secondary market) of a product or service life cycle (Ben Yahia *et al.* 2017). RePtSCs are linked with maintenance support functions that aims to

ensure RePts are available and compatible when required to derive value from instances of maintenance, upgrade, repair, reconditioning, and overhaul (Teixeira *et al.* 2018). Additionally, stocked RePts are deemed as idle capital locked up, in a combination of storage cost and the forward, or reverse, logistics required to restore a product's functionality (Molenaers *et al.* 2012). Consequently, concepts of digital RePt and on-demand RePt production using AM is seen as probably to address these RePt challenges (Holmström *et al.* 2010). Due to expected through-life-value arising from products or services that are designed to be maintained, Original Equipment Manufacturers (OEMs) and IP owners frequently attempt to maintain a controlling interests in producing and distributing their protected product or service, extending this influence to producing, stocking, distributing, and selling RePts needed to operate their product (Götting and Hetmank 2019). Furthermore, RePtSC are often embattled with competing interests from both benevolent and malevolent actors who may introduce genuine or counterfeit RePts respectively to tap into OEMs clientele market share (Drexel 2008, Beldiman and Blanke-Roeser 2017). Scholars and practitioners highlight AM's unique disruptive capability to favour simplifying complex SC, increase asset uptime, reducing inventory and lead time, inevitably improve SC performance and sustainability especially towards use cases for RePts (Holmström and Partanen 2014, Knofius *et al.* 2019). Nevertheless, concerns arise on AM skillset, AM knowhow and AM quality assurance, also its ability to democratise manufacturing, compounds existing issues of local and global product market challenges with rising IP infringements and data breaches; despite legislative efforts made to combat these socially undesirable actions (Xiong and Lagerström 2019, IP Crime Group 2021).

Few studies have looked specifically into management aspects on IP of AM for RePtSC to contribute towards gaining an understanding of the complexities that exist in these fields. Examples include: Geissbauer *et al.* (2017) surveyed experts views on future of AM for RePt to suggest RePt IP would be traded rather than physical RePt. This was followed by Ballardini *et al.* (2018) investigating IP, technology and business issues affecting growth in AM use in RePtSC within industrial settings, while Kim *et al.* (2019) explored use of digital RePt libraries to inspect component damage and make RePt on-demand using AM via their maintenance framework. Meanwhile, Boer *et al.* (2020) and Salmi *et al.* (2020), examined potentials for AM to make RePt during emergencies like COVID-19, humanitarian, or military missions. Furthermore, Holland *et al.* (2018) described their AM transactions on secure networks; thus, mitigating IP compromise risks; whereas Zhang *et al.* (2021) studied IP licensing for AM use to produce RePts from OEM perspectives. Also, Kostidi *et al.* (2021) and Wooldridge *et al.* (2020) considered AM for RePts in industries like oil and gas and maritime to determine both viability and limitations.

These studies demonstrate efforts to understand different aspects of securing IP against compromise and the mitigation of compromised IP reception as an added responsibility to multiple AM actors in RePtSCs. We argue that there is more value in collaboratively examining IP management concerns

effect on AM, SC, and RePt to gain deeper insights into its issues. Individuals and organisations must understand IP implications for AM use in RePtSC, to avoid encountering legal battle like IP litigation or liability; by knowing if AM is "IP suitable" for RePt making or servicing, especially when scanning a part to reproduce for personal or commercial gains. Two recent examples: one OEM ordered massive takedowns of AM digital models of their RePt from public online repositories (Stumpf 2022a); meanwhile, another OEM availed tons of AM digital models of their RePt via public online repositories (Stumpf 2022b). Undoubtedly, AM use in RePtSCs presents itself as a promising application under I4.0; however, consistent concerns exist about its IP management and control implications, which unfortunately remains not well understood. Based on the AM, SC, IP, and RePt interrelations, this paper aims to clarify the relative importance of IP compromise issues perceived by practitioners and academics for AM application within RePtSC from a holistic management perspective. The remainder of this paper is structured as follows: *Section 2* reveals methodological approaches; *Section 3* presents findings; *Section 4* discusses outcomes and concludes.

## 2. APPROACH AND METHOD

A questionnaire was developed, using the Qualtrics platform, and delivered to each participant (industry and academia) over series of online web meetings, using MS Teams. The guided online delivery facilitated additional explanations, answering pertinent questions by participants, and encouraged dedicated time to work on the data collection task. With ethical approval granted, the questionnaire was reviewed, piloted, and adjusted. Response rate to all questions was about 70% during pilot sessions; however, response rate increased to 96–100% during live sessions (the few missed responses were due to internet issues or human oversight errors).

This study focused on participants with knowledge and experiences of AM, IP, SC and RePt. Participants were recruited via purposive sampling approach by peer referrals and online profile searching on LinkedIn to reach relevant candidates (Bryman and Bell 2019). A total of 26 participants took part in this activity. Each participant was randomly presented two, out of three, dedicated RePtSC scenarios to evaluate. Afterwards, responses were requested for our Likert type questionnaire on hypothetical security concern statements, that measure their IP concern levels in the context of each presented scenario. This created equal consideration opportunity for all scenarios and mitigated uninformed responses that affect response reliability (de Leeuw *et al.* 2009). The questions asked were:

*With respect to the scenario of Additive Manufacturing application for Replacement-Parts within the Supply Chain, how concerned are you about the following issues with regards to Intellectual Property compromise?*

Relevant literature that interrelates our area of study were reviewed to provide theoretical blueprints for deriving question sets that navigate critical gaps and recurring issues raised by scholars within this multidisciplinary research field (Alvesson and Sandberg 2013, O'Leary 2017). The derived

questions, used to obtain participants responses, were grouped into four statements sets (AM, IP, SC and RePt issues).

AM questions set was deduced from the works of scholars like Yampolskiy *et al.* (2018) and Graves *et al.* (2019). The questions set under AM issues entailed concerns about: *Data*: AM data exchange being intercepted or misused. *Equipment*: AM equipment being hacked or attacked. *Material*: AM material properties being exposed or tampered. *Process*: AM process parameters being divulged or extracted.

SC questions set was deduced from the works of scholars like Fadhel *et al.* (2014) and Gupta *et al.* (2020). The questions set under SC issues entailed concerns about: *Confidentiality*: SC confidentiality agreements being breached or exposed. *Integrity*: SC integrity trust being broken or weakened. *Provenance*: SC provenance verification being lost or inaccessible.

IP questions set was deduced from the works of scholars like Brown *et al.* (2016) and Flank (2017). The questions set under IP issues entailed concerns about: *Theft*: IP information or knowledge being stolen. *Misuse*: IP information or knowledge being used without approval. *Adulteration*: IP information or knowledge being unknowingly tweaked, modified, and mixed.

RePt questions set was deduced from the works of scholars like Chekurov *et al.* (2018) and Chaudhuri *et al.* (2021). The questions set under SC issues entailed concerns about: *Obsolete*: RePt becoming or remaining obsolete. *Maintainable*: RePt maintainability purposes becoming void or invalid. *Incompatible*: RePt being incompatible for its target function or system.

Overall, these group of questions above were asked to obtain empirical data from different perspectives about IP compromise concerns with respect to scenarios of AM, IP, SC and RePt combined. Participants were asked to respond based on a Likert type scale 1-5 with the categorization: 1=*Not Concerned* (NoC), 2=*Slightly Concerned* (SIC), 3=*Moderately Concerned* (MoC), 4=*Very Concerned* (VeC) and 5=*Extremely Concerned* (ExC). The Likert scale type of questions was deemed apt to the task to measure subjective views like attitude, perception towards statements, or situations that is not easily quantified; moreover, it provides an avenue for transformation into a quantitative format for further aggregate processing of results (Bryman and Bell 2019). Collated results were normalized in analysis to determine the percentage of participants views and weighted averages calculated on each issue to determine the significant issues; thus, indicates concern levels on IP of AM use within RePtSC, as tabulated results presented in the next section. Additionally, the ordinal category scores are combined with the collated responses for each category to obtain Weighted Average (WAvg) as an unbiased way of determining rankings. Finally, a comparison between high sentiments (VeC to ExC) and low sentiments (SIC to NoC) was calculated by generating a ratio of high sentiments to low sentiments and termed as High-Low (HiLo) for differentiation. High-level response correlations were performed on each issue and sentiment category to quickly explore emerging cross-mapped patterns that may support discussions on their interconnected nature.

### 3. RESULTS AND FINDINGS

Participants contributed mainly from roles of Management (Executive, Strategy, Technology, Manufacturing), Engineering (Research, Manufacturing and Design), and Academic in descending order. Participants’ collective responses to questions about scenarios presented to them are presented as concern issues relating to: AM (see Table 1), SC (see Table 2), IP (see Table 3) and RePt (see Table 4). Each table has a response distribution in percentages (%), while WAvg scores and HiLo sentiments are dimensionless metrics. Results from Table 1-Table 4 suggests all AM, IP, SC and RePt issues are significant concern areas for participants, but sentiments are perceived at varied levels from MoC to VeC.

From Table 1, *AM data* was identified as the principal concern, based on its HiLo being strongly dominated by VeC and ExC sentiments. *AM process* was the second concern area; however, its HiLo was slightly tipped in favour of SIC and NoC sentiments. *AM materials* and *AM equipment* were closely ranked as the third and fourth concern areas respectively; assessed by their respective HiLo which were both dominated by SIC and NoC sentiments. Among ExC sentiments, *AM data* was the most represented issue, thus confirming its importance; meanwhile *AM equipment* and *AM process* comprised the most represented issues among NoC sentiments, confirming *AM equipment* as the least ranked issue, suggests subaltern perception on equipment compromise risks and *AM process* being in tension between strong and weak sentiments on process repeatability challenges influence on perceived compromise risks. Each AM issue’s results, supported by their respective WAvg scores, suggests participants’ collective significance and concern levels range from MoC to VeC sentiments. Finally, Table 1 results demonstrate a ranked concern level pattern containing *AM equipment*, *AM materials*, *AM process* and *AM data* in ascending order.

**Table 1. Concerns related to Additive Manufacturing**

Concerns & Scores	Additive Manufacturing Issues			
	Data	Equipment	Materials	Process
5 ExC	23%	4%	12%	8%
4 VeC	44%	19%	15%	25%
3 MoC	23%	40%	35%	33%
2 SIC	6%	29%	32%	26%
1 NoC	4%	8%	6%	8%
HiLo	6.70	0.62	0.71	0.97
WAvg	3.76	2.82	2.95	2.99

From Table 2, *SC confidentiality* was identified as the principal concern, based on its HiLo being strongly dominated by VeC and ExC sentiments. *SC integrity* and *SC provenance* were closely ranked as the second and third concern areas respectively; assessed by their respective HiLo which were both dominated by VeC and ExC sentiments. Among ExC sentiments, *SC confidentiality* was the most represented issue, thus confirming its importance; meanwhile *SC integrity* and *SC provenance* comprised zero represented issues among NoC sentiments, which suggest these are SC issues that participants share interrelated sentiments on their compromise, especially with visibility loss on SC tiered activities and actors involved

in the overall process. Each SC issue's results, supported by their respective WAvG scores, suggests participants' collective significance and concern levels range from SIC to VeC sentiments. Finally, Table 2 results demonstrate a ranked concern level pattern containing *SC provenance*, *SC integrity* and *SC confidentiality* in ascending order.

**Table 2. Concerns related to Supply Chain**

Concerns & Scores	Supply Chain Issues		
	Confidentiality	Integrity	Provenance
5 ExC	17%	12%	13%
4 VeC	29%	42%	23%
3 MoC	40%	25%	47%
2 SIC	12%	21%	17%
1 NoC	2%	0%	0%
HiLo	3.29	2.57	2.12
WAvG	3.47	3.45	3.32

From Table 3, *IP adulteration*, *IP theft* and *IP misuse* were closely ranked as the first, second and third concern areas respectively; assessed by their respective HiLo which were dominated by VeC and ExC sentiments; additionally, WAvG was considered as an assessment tie breaker for HiLo similarities. Among ExC sentiments, *IP adulteration* was the most represented issue, thus confirming its importance; meanwhile *IP theft*, *IP misuse* and *IP adulteration* comprised equally represented issues among NoC sentiments which suggest these are IP issues that participants share interrelated sentiments on their compromise, especially multiple instances of involvement as an effector, recipient, or victim of active and passive infringement activities. Each IP issue's results, supported by their respective WAvG scores, suggests participants' collective significance and concern levels range from MoC to VeC sentiments. Finally, Table 3 results demonstrate a ranked concern level pattern containing *IP misuse*, *IP theft* and *IP adulteration* in ascending order.

**Table 3. Concerns related to Intellectual Property**

Concerns & Scores	Intellectual Property Issues		
	Theft	Misuse	Adulteration
5 ExC	17%	16%	22%
4 VeC	46%	47%	42%
3 MoC	25%	25%	24%
2 SIC	10%	10%	10%
1 NoC	2%	2%	2%
HiLo	5.25	5.25	5.33
WAvG	3.66	3.65	3.72

From Table 4, *Incompatible RePt* was identified as the principal concern, based on its HiLo being strongly dominated by VeC and ExC sentiments. *Maintainable RePt* was the second concern area; similarly, based on its HiLo being dominated by VeC and ExC sentiments. *Obsolete RePt* was the third concern area; likewise, based on its HiLo being dominated by VeC and ExC sentiments. Among ExC sentiments, *incompatible RePt* was the most represented issue, thus confirming its importance; meanwhile *maintainable RePt* comprised the most represented issues among NoC sentiments, suggesting tensions between RePt repair or remake capabilities and unclear freedom to operate connotations. Each RePt issue's results, supported by their respective WAvG

scores, suggests participants' collective significance and concern levels range from MoC to VeC sentiments. Finally, Table 4 results demonstrate a ranked concern level pattern containing *Obsolete RePt*, *Maintainable RePt* and *Incompatible RePt* in ascending order.

**Table 4. Concerns related to Replacement Part**

Concerns & Scores	Replacement Part Issues		
	Obsolete	Maintainable	Incompatible
5 ExC	4%	12%	21%
4 VeC	31%	35%	29%
3 MoC	38%	27%	25%
2 SIC	15%	13%	15%
1 NoC	12%	13%	10%
HiLo	1.30	1.81	2.00
WAvG	3.00	3.20	3.36

The next section briefly discusses these results by reflecting on the literature about IP of AM for RePtSC, to get a better understanding on this I4.0 capability.

#### 4. DISCUSSION AND CONCLUSION

The data trends from Table 1-Table 4 reveal popular views ranging from MoC to VeC for most issue categories; however, IP and RePt issues demonstrated the highest popular views in VeC, which interestingly aligns with our study's enquiry on understanding IP compromise concern levels. An analysis on the average of respective averages under each issue category (AM, IP, SC, RePt) revealed: IP issues were the highest ranked score (3.68), followed by SC issues as the second ranked score (3.41), then RePt issues as the third ranked score (3.19), and finally AM issues as the fourth ranked score (3.13). The findings suggest that despite the much-anticipated opportune benefits associated with AM use for RePt within SC; there remains a consensus among participants about IP compromise being a significant concern through the issues enlisted in this and other studies like that of Brown *et al.* (2016). Undoubtedly, benefits on IP of AM use for RePt within SC exists like on-demand manufacturing, augmented distributed supply networks, value trading in intellectual digital creations, and repair or remake obsolete components; nevertheless, these applications also inherit challenges associated with each concept strand involved that makes the issue more complex than handling them via individual functions as stated by Ballardini *et al.* (2018).

Each issue category's average of average score was further inspected to derived inferable explanations. It was discovered that IP issues (3.68) and SC issues (3.41) were closely scored, thus suggesting probable linkages to coordination issues flagged by Flank (2017) and Gupta *et al.* (2020) as areas that can be easily overlooked for existing structural functions; but attentively needs a holistic approach towards managing IP challenges especially with application cases of RePtSC within I4.0. Meanwhile, AM issues (3.13) and RePt issues (3.19) were closely scored, thus suggesting links between ongoing challenges and opportunities of AM use for RePts, where despite the technical feasibility of redesigning RePts for manufacture or service with AM under license, the process could also introduce IP conflicts between getting the job done and undertaking due diligence to ensure one is not at risk of

overreaching allowable IP usage or exemptions. Not forgetting the technical effect on IP compromise from AM system manipulation and resultant effect on cases like *incompatible RePts* as highlighted by Graves *et al.* (2019) and Chaudhuri *et al.* (2021) on what is often referred to as IP embedded technical data (including digital RePt inventories within online repositories).

Another inferred explanation to the results suggests that participants may have been concerned about IP exemptions and creative adulterations. These practices have succeeded; yet, they have been challenging within digital copyright, and it is uncertain what they could mean for AM digital model data and AM process parameters. *IP theft* is a popular concern in literature; however, this study's results reveal more concerns about *IP adulteration* and *IP misuse*. This concern finds its validity especially with IP being intangible, like know-how or trade secrets about AM process parameter or AM material ingredients involved; meanwhile visibility within SCs remains a challenge, so this concern may align towards potential instances of deceptive overproduction runs, despite existing contractual agreements as highlighted by Holland *et al.* (2018).

Additionally, an interesting discovery about participants expressing no NC sentiments about *SC integrity* and *SC provenance* links back to discussions on IP and SC visibility issues of trust. Trust with not only the SC actors but also the integrity of *AM data* or an AM component being made; therefore, plausibly justifying some business practices, as in the aerospace or oil and gas industry to engage only qualified SC actors in a bid to manage and control IP as a community mechanism strategy. We deem collaborative approaches that avoid stifling innovation as better suited for IP sustenance, because I4.0 extends AM towards more decentralized approaches, so centralized exclusion IP management practices are strongly challenged with increased AM adoption (UK Additive Manufacturing Steering Group 2017).

Another discovery was the sentiments towards *AM materials* and *AM equipment* being less strong despite literature in that field of AM security highlighting potential vulnerabilities for multiple compromises include *IP theft* and *IP adulteration* being facilitated. Nevertheless, this could suggest that AM material and equipment providers may either have strong systems in place that keeps their IP intact due to the rate of AM technology advancements and key IP expiries. Alternatively, it could also mean the participants often perceived and trust AM systems and AM feedstock are locked down and not necessarily open on public networks for the anticipated IP compromise; thus, speculating their low sentiments expressed. Nevertheless, this could find concurrence in practice with existing digital RePts, by perceiving future RePt IP trade via licensing models like those explored by Zhang *et al.* (2021).

Our generated contingency matrices explored correlated response categories to reveal interesting patterns among sentiments. VeC was the only sentiment linked to all highest frequencies in each matrix. *SC integrity* was the most matched issue against *AM data*, *IP theft*, *IP misuse* and *maintainable RePt*. Followed by *IP theft* which uniquely matched against *AM data* and *maintainable RePt* issues. Meanwhile, *AM data* uniquely matched *maintainable RePt*. Finally, *obsolete RePt*

and *SC provenance* emerged as exclusively matched issues. We suggest these correlated patterns depict our previously raised uncertainties about SC visibility and mistrust among actors, with potential for wrongfully acquired or utilisation of value-embedded IP. Coupled with digital or physical AM data security concerns about on-demand RePt make and repair quality. Evidently, these top issues are perceived as highly interconnected and require holistic approaches to tackle them.

This paper contributes insights to management understanding and practice prioritization with empirically quantified data that provides perspectives on critical areas of concern about securing IP against compromises for AM applications within RePtSCs. This can support practitioner efforts in prioritizing management and control efforts towards securing IP, as well as guide further research activities. A major limitation we identify is with our study's sample size being challenged for generalization. Nevertheless, this would suffice for our level of exploratory investigation being backed by issues extracted from literature; thus, creates avenues for future research agendas. Future research could focus on the following: raising wider questions for gaining understanding on the situational context behind participants' choices to elucidate motives; extending data collection outreach for larger and more varied participants sample sizes to strengthen correlated patterns and overall generalization; investigating strategies involved for managing and controlling IP of AM applications within SC, including unique case of RePts to facilitate AM adoption.

#### ACKNOWLEDGEMENT

This paper contains research that is part of the lead author's PhD, supervised by a team including all co-authors, and supported by a scholarship from University of Strathclyde. We would like to thank other members of the PhD supervision team: Angela Daly and Graeme McLaughlin.

#### REFERENCES

- Alvesson, M. and Sandberg, J., 2013. Constructing Research Questions: Doing Interesting Research. London: SAGE Publications Ltd.
- Anusci, V., 2018. Gartner's Top 3 Failed Predictions on 3D Printing (That Will Probably Never Come True) [online]. [www.3dprintingmedia.network](http://www.3dprintingmedia.network). Available from: <https://www.3dprintingmedia.network/gartners-top-3-predictions-3d-printing-not-come-true-probably-never-will/> [Accessed 17 Oct 2018].
- Ballardini, R.M., Flores Ituarte, I., and Pei, E., 2018. Printing spare parts through additive manufacturing: legal and digital business challenges. *Journal of Manufacturing Technology Management*, 29 (6), 958–982.
- Beldiman, D. and Blanke-Roeser, C., 2017. An International Perspective on Design Protection of Visible Spare Parts. Cham: Springer International Publishing.
- Birtchnell, T., Daly, A., Rayna, T., and Striukova, L., 2018. 3D Printing and Intellectual Property Futures.
- Boer, J. den, Lambrechts, W., and Krikke, H., 2020. Additive manufacturing in military and humanitarian missions: Advantages and challenges in the spare parts supply chain. *Journal of Cleaner Production*, 257, 120301.
- Brown, A., Yampolskiy, M., Gatlin, J., and Andel, T., 2016. Legal Aspects of Protecting Intellectual Property in Additive Manufacturing. In: M. Rice and S. Sheno, eds. *Critical Infrastructure Protection X*. Arlington: Springer International Publishing, 63–79.
- Bryman, A. and Bell, E., 2019. *Social Research Methods*. 5th ed. Don Mills: Oxford University Press Canada.

- Chaudhuri, A., Gerlich, H.A., Jayaram, J., Ghadge, A., Shack, J., Brix, B.H., Hoffbeck, L.H., and Ulriksen, N., 2021. Selecting spare parts suitable for additive manufacturing: a design science approach. *Production Planning & Control*, 32 (8), 670–687.
- Chekurov, S., Metsä-Kortelainen, S., Salmi, M., Roda, I., and Jussila, A., 2018. The perceived value of additively manufactured digital spare parts in industry: An empirical investigation. *International Journal of Production Economics*, 205, 87–97.
- Chhetri, S.R., Faezi, S., Rashid, N., and Al Faruque, M.A., 2018. Manufacturing Supply Chain and Product Lifecycle Security in the Era of Industry 4.0. *Journal of Hardware and Systems Security*, 2 (1), 51–68.
- Drexler, J., 2008. *Research Handbook on Intellectual Property and Competition Law*. Edward Elgar Publishing.
- Drissen, M., Arts, J., Van Houtum, G.J., Rustenburg, J.W., and Huisman, B., 2014. Maintenance spare parts planning and control: a framework for control and agenda for future research. *Production Planning & Control*, 26 (5), 407–426.
- European Commission, 2004. Proposal for a Directive of the European Parliament and of the Council: amending Directive 98/71/EC on the legal protection of designs. Brussels.
- Fadhel, N.F., Crowder, R.M., Akeel, F., and Wills, G.B., 2014. Component for 3D printing provenance framework: Security properties components for provenance framework. In: *World Congress on Internet Security (WorldCIS-2014)*. IEEE, 91–96.
- Flank, S., 2017. Legal Issues in IP Protection for Additive Manufacturing. *Texas A&M Journal of Property Law*, 4 (1), 1–14.
- Geissbauer, R., Wunderlin, J., and Lehr, J., 2017. The future of spare parts is 3D: A look at the challenges and opportunities of 3D printing.
- Götting, H.-P. and Hetmank, S., 2019. The scope of patent protection for spare parts and its extension through other tools of intellectual property. In: T. Takenaka, ed. *Research Handbook on Patent Law and Theory*. Cheltenham: Edward Elgar Publishing, 239–249.
- Graves, L.M.G., Lubell, J., King, W., and Yampolskiy, M., 2019. Characteristic Aspects of Additive Manufacturing Security From Security Awareness Perspectives. *IEEE Access*, 7, 103833–103853.
- Gupta, N., Tiwari, A., Bukkapatnam, S.T.S., and Karri, R., 2020. Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks. *IEEE Access*, 8, 47322–47333.
- Holland, M., Stjepandić, J., and Nigischer, C., 2018. Intellectual Property Protection of 3D Print Supply Chain with Blockchain Technology. In: 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC). Stuttgart: IEEE, 1–8.
- Holmström, J. and Partanen, J., 2014. Digital manufacturing-driven transformations of service supply chains for complex products. *Supply Chain Management: An International Journal*, 19 (4), 421–430.
- Holmström, J., Partanen, J., Tuomi, J., and Walter, M., 2010. Rapid manufacturing in the spare parts supply chain. *Journal of Manufacturing Technology Management*, 21 (6), 687–697.
- Hornick, J., 2015. 3D Printing and IP Rights: The Elephant in the Room. *Santa Clara Law Review*, 55 (4), 801–820.
- IP Crime Group, 2021. *IP Crime and Enforcement report 2020/21*. Newport.
- Kim, H., Cha, M., Kim, B.C., Lee, I., and Mun, D., 2019. Maintenance Framework for Repairing Partially Damaged Parts Using 3D Printing. *International Journal of Precision Engineering and Manufacturing*, 20 (8), 1451–1464.
- Knofius, N., van der Heijden, M.C., and Zijm, W.H.M., 2019. Consolidating spare parts for asset maintenance with additive manufacturing. *International Journal of Production Economics*, 208, 269–280.
- Kostidi, E., Nikitakos, N., and Progoulakis, I., 2021. Additive Manufacturing and Maritime Spare Parts: Benefits and Obstacles for the End-Users. *Journal of Marine Science and Engineering*, 9 (8), 895.
- de Leeuw, E.D., Hox, J., and Dillman, D., 2009. *International Handbook of Survey Methodology*. New York: Psychology Press.
- Mcdermott, K.C., Winz, R.D., Hodgson, T.J., Kay, M.G., King, R.E., and Mcconnell, B.M., 2021. Performance tradeoffs for spare parts supply chains with additive manufacturing capability servicing intermittent demand. *Journal of Defense Analytics and Logistics*, 5 (2), 179–213.
- Mendis, D., Nordemann, J.B., Ballardini, R.M., Brorsen, H., Moreno, M. del C.C., Robson, J., and Dickens, P., 2020. *The Intellectual Property Implications of the Development of Industrial 3D Printing*. Brussels: European Union.
- Molenaers, A., Baets, H., Pintelon, L., and Waeyenbergh, G., 2012. Criticality classification of spare parts: A case study. *International Journal of Production Economics*, 140 (2), 570–578.
- O’Leary, Z., 2017. *The Essential Guide to Doing Your Research Project*. 3rd ed. London: SAGE Publications Ltd.
- Ocean Tomo, 2017. *Intangible Asset Market Value*. Chicago.
- Petrick, I.J. and Simpson, T.W., 2013. 3D Printing Disrupts Manufacturing: How Economies of One Create New Rules of Competition. *Research-Technology Management*, 56 (6), 12–16.
- Salmi, M., Akmal, J.S., Pei, E., Wolff, J., Jaribion, A., and Khajavi, S.H., 2020. 3D Printing in COVID-19: Productivity Estimation of the Most Promising Open Source Solutions in Emergency Situations. *Applied Sciences*, 10 (11), 4004.
- Santoso, S.M. and Wicker, S.B., 2016. The future of three-dimensional printing: Intellectual property or intellectual confinement? *New Media & Society*, 18 (1), 138–155.
- Stumpf, R., 2022a. Honda Orders Big Takedown of Honda-Related 3D Printing Models From Maker Communities [online]. *The Drive*. Available from: <https://www.thedrive.com/news/honda-orders-big-takedown-of-honda-related-3d-printing-models-from-maker-communities> [Accessed 22 Apr 2022].
- Stumpf, R., 2022b. Ford Releases Blueprint Files for Tons of 3D-Printable Maverick Accessories [online]. *The Drive*. Available from: <https://www.thedrive.com/news/44276/ford-releases-blueprint-files-for-tons-of-3d-printable-maverick-accessories> [Accessed 23 Mar 2022].
- Teixeira, C., Lopes, I., and Figueiredo, M., 2018. Classification methodology for spare parts management combining maintenance and logistics perspectives. *Journal of Management Analytics*, 5 (2), 116–135.
- UK Additive Manufacturing Steering Group, 2017. *Additive Manufacturing UK (AM-UK): National Strategy 2018-25*. Conventry.
- Weinberg, M., 2016. When 3D Printing and the Law Get Together, Will Crazy Things Happen? In: B. van den Berg, S. van der Hof, and E. Kosta, eds. *3D Printing*. The Hague: T.M.C. Asser Press, 11–35.
- Wohlers Associates, 2021. *Wohlers Report 2021*. Fort Collins: Wohlers Associates.
- Wooldridge, M., Wangenheim, C., Herberg, W., and Wettmarshausen, T., 2020. Applications of Metal Additive Manufacturing in the Oil and Gas Industry. In: *Offshore Technology Conference*. Houston: OTC.
- Xiong, W. and Lagerström, R., 2019. Threat modeling – A systematic literature review. *Computers & Security*, 84, 53–69.
- Ben Yahia, W., Ayadi, O., and Masmoudi, F., 2017. A fuzzy-based negotiation approach for collaborative planning in manufacturing supply chains. *Journal of Intelligent Manufacturing*, 28 (8), 1987–2006.
- Yampolskiy, M., King, W.E., Gatlin, J., Belikovetsky, S., Brown, A., Skjellum, A., and Elovici, Y., 2018. Security of additive manufacturing: Attack taxonomy and survey. *Additive Manufacturing*, 21 (November 2017), 431–457.
- Zhang, Y., Westerweel, B., Basten, R.J.I., and Song, J.-S.J., 2021. Distributed 3D Printing of Spare Parts via IP Licensing. *SSRN Electronic Journal*.