Terabytes and 2x4s:
The Benefits (and Potential Risks) of Automated/Remotely Operated Technology in the Construction Industry

Christopher S. Drewry and Jeffrey M. Kraft[1]
DREWRY SIMMONS VORNEHM, LLP
736 Hanover Place, Suite 200
Carmel, IN 46032

[1] *Christopher S. Drewry is a partner with the law firm of Drewry Simmons Vornehm, LLP, in Indiana (www.dsvlaw.com). He focuses his practice on construction law and litigation, as well as labor and employment law and litigation. He is currently the Chair of the Construction Law and Litigation Committee of the International Association of Defense Counsel. He can be reached at cdrewry@dsvlaw.com.*

Jeffrey M. Kraft is an associate at Drewry Simmons Vornehm, LLP, where he focuses his practice on general litigation, including construction law. He can be reached at jkraft@dsvlaw.com.

As with many industries, the rapid advance of automated and remotely operated technologies has impacted, and will continue to impact, the construction industry in various significant ways. These new technologies offer a number of advantages to project participants, including the potential for substantial increases in efficiency, coordination, and safety. However, while the benefits are potentially limitless, they also introduce the possibility for new risks and exposure to liabilities which current risk management regimes may not adequately address in their current form. While far from comprehensive, this article will briefly review the potential benefits and risks posed by three new areas of technology impacting the construction industry, specifically (1) unmanned aircraft systems (UAS), (2) the internet of things, and (3) 3D-printing.

I. Unmanned Aircraft Systems (UAS)

More commonly called drones, UAS have seen rapid growth in use across a variety of sectors, from aerial photography and security surveillance to fast food delivery. The Federal Aviation Administration (FAA) estimates that UAS in use in the United States increased from approximately 2.5 million in 2016 to more than 7 million in 2020, which is approximately 10 times the number of manned aircraft registered in the U.S. The construction industry accounts for a significant portion of this increased use.[2]

A. <u>Potential Benefits</u>

UAS are used primarily for data collection. Armed with a variety of increasingly small, lightweight, and inexpensive sensors, UAS can collect and transmit data regarding light, images, sounds, magnetic fields, heat, and chemical molecules.[3]

Their versatility at data collection has broad application in the construction industry. On site, UAS can perform surveys and inspections, provide security surveillance and progress reports, identify safety issues, orient new employees, augment reality, and otherwise aid in coordinating, managing, and monitoring site activities and logistics. UAS also can improve safety by performing tasks that would expose a human worker to risk of harm. In addition, UAS can aid in pre- and post-construction activities such as design, engineering, planning, and marketing. Furthermore, UAS use can significantly reduce labor costs. One estimate values the labor and services exposed to replacement by UAS at $127.3 billion worldwide, one third of which comes from the construction and infrastructure industries.[4]

---

[2] Jennifer Trock, et al., *The Use of Unmanned Aircraft Systems in the Construction Industry in the United States and Canada: An Overview of the Applicable Frameworks*, 12 No. 1 ACCLJ 4 (Jan. 2018).
[3] *Id*.
[4] *Id*.; Daniel S. Brennan, *The Internet of Things in Construction: Opportunity, Risk and Insurance Considerations*, 13 No. 2 ACCLJ 3 (Summer 2019).

B. Potential Risks/Liabilities

Along with the potential benefits discussed above, UAS present three particular areas of potential risk and liability: compliance with government regulation, operational risks, and insurance coverage issues.

1. Compliance with Government Regulations

The primary federal regulations governing the use of UAS is 14 C.F.R. § 107, which applies to commercial UAS under 55 lbs. Section 107 requires that commercial UAS operators obtain a Remote Pilot Certificate. Notably, obtaining a Remote Pilot Certificate does not require any experience operating UAS. Rather, the applicant must: (a) be at least 16 years old; (b) speak and write English; (c) possess the physical and mental fitness to safely operate UAS; (d) pass an aeronautical knowledge test; and (e) pass vetting by the Transportation Safety Administration (TSA).[5]

In addition to requiring a Remote Pilot Certificate for operators, Section 107 imposes several restrictions on UAS use, including: (a) maintaining visual-line-of-sight (VLOS) with the UAS at all times; (b) operating at speeds no greater than 100 mph; (c) operating at altitudes no greater than 400 feet or farther than 400 feet of a structure; (d) operating only during daylight hours; (e) not operating in controlled airspace without prior air traffic control approval; (f) yielding the right-of-way to manned aircraft; (g) not operating from a moving vehicle or aircraft; (h) not operating under the influence of alcohol or drugs; (i) not operating multiple UAS simultaneously; and (j) not flying over the general public. Operators may apply with the FAA for waiver of many of these restrictions. However, waivers may come with a new set of restrictions. For example, to obtain waiver of the daylight-operations restriction, applicants must demonstrate how they will: (a) maintain VLOS with the UAS; (b) avoid other aircraft, structures, people, and other obstacles; (c) continually determine the altitude, attitude, and movement of the UAS; (d) ensure all participants can recognize and overcome visual illusions and physiological conditions that may degrade night vision; and, (e) enable the UAS to be seen at a distance of three miles, unless another system is already in place for avoiding all non-participating aircraft.[6]

Failure to comply with these regulations presents a substantial risk to operators. The FAA has broad authority to enforce these regulations with warning notices, letters of correction, and civil penalties. This latter option can be costly to violators; companies may be fined up to $34,777 per violation, per day, while individuals may be fined up to $1,527. In addition, the FAA may impose criminal sanctions for purposeful and significant violations.[7]

---

[5] Trock, *supra* note 1; 14 C.F.R §§ 107.53-107.79 (2016).
[6] Trock, *supra* note 1; 14 C.F.R. §§ 107.11-107.51, 107.200-107.205 (2016).
[7] Trock, *supra* note 1; 14 C.F.R. § 13.301 (2021).

2. Operational Risks

As one might expect from a 55-lbs. flying object with spinning metal blades, UAS present a significant risk for personal injury and/or property damage through malfunction or operator error. This risk is magnified when operating in the context of a busy construction site filled with ever-moving, ever-changing people, machines, and other obstacles. The risk is increased further by the minimal requirements for obtaining a Remote Pilot Certificate, which allows for commercial UAS operation by largely inexperienced pilots. Construction industry members may be advised to set (and insurers may require) additional safety requirements for UAS operation, such as minimum flight hours for operators or mandatory recovery parachutes. In addition, as discussed further in the context of the Internet of Things below, UAS operation is vulnerable to cyberattack.[8]

3. Insurance Coverage Issues

Although currently not required by law, UAS insurance coverage may be required by specific clients or projects, and most credible commercial operators carry UAS liability insurance coverage. Significantly, because commercial general liability insurance policies usually contain aviation exclusions, they generally do not cover liability arising out of UAS operation. Construction industry members wishing to employ UAS will want to pursue either adding UAS coverage to their existing policies or purchasing separate commercial UAS insurance, which typically will cover aircraft operations (including non-pilot, on-ground crew), manufacturer product liability, third-party legal liability, premises liability, medical payments, fire, independent contractor's liability, personal injury, advertising liability, contractual liability, and fellow employee coverage. In exchange, insurers typically require commercial UAS operators to adhere to additional safety measures (such as minimum operator experience levels) beyond the FAA requirements.[9]

II. The Internet of Things

Unlike UAS, the Internet of Things (IOT) is not a single, tangible type of new technology. Rather, it refers to the interconnectivity of smart devices. In addition to smart phones and tablets, these smart devices can include UAS, personal wearable devices, remotely operated or autonomous vehicles and machinery, and site access, security, or control systems.[10]

[8] Trock, *supra* note 1; Brennan, *supra* note 3.
[9] Trock, *supra* note 1.
[10] Brennan, *supra* note 3.

A. Potential Benefits

The IOT offers virtually limitless potential to the areas of efficiency and safety in the construction context. In addition to the potential benefits of UAS discussed above, these potential benefits include: (a) remote/autonomous operation of vehicles, hoists, and other construction equipment; (b) tracking equipment location, use, idle time, and maintenance alerts; (c) tracking worker time, location, movements, and fatigue level; (d) automatic alert systems (for example, to alert a reversing vehicle operator of a potential collision, restrict machinery operation when a worker is within a certain distance, or alert workers when they enter a pre-defined danger zone); and (e) increased site security through the use of biometric security systems.[11]

B. Potential Risks/Liabilities

As discussed in the context of UAS above, construction equipment and devices connected by the IOT present a risk of personal injury or property damage through malfunction or operator error. However, due to the inherent interconnectivity of these devices, the IOT also presents the unique risk of vulnerability to cyberattack and associated insurance coverage issues.

1. Cyberattack Risks

Like malfunction or operator error, cyberattacks on devices connected by the IOT can result in bodily injury or property damage. UAS or other remotely controlled vehicles can be hijacked, control systems on hoists can be overridden, and failsafe systems can be disabled, all of which could lead to catastrophic harm. In addition, interference with project management systems can result in significant business losses from project delays. Corruption of these systems can also lead to unauthorized disclosure of private or confidential information, such as workers' protected personal identifying information or project information protected by intellectual property law or contractual confidentiality provisions.[12]

2. Cyberattack Insurance Coverage Issues

Many carriers offer cyber insurance, which typically covers both the insured's first-party losses and third-party claims arising out of cyberattacks. First-party coverage generally includes: (a) data asset protection; (b) remediation costs; (c) business interruption coverage; (d) cyber extortion coverage; and (e) crisis management and response costs. Third-party coverage typically includes losses incurred by third parties for: (a) unauthorized disclosure, use, or destruction of confidential information or protected personal information; (b) denied or delayed access to the cyberattacked entity's systems; (c) transmission of malicious code or malware from the cyberattacked entity's systems; and (d) copyright infringement, misappropriation of trade secrets, defamation, or invasion of privacy. Third-party coverage typically also covers defense costs for

[11] *Id.*
[12] *Id.*

any legal proceeding against the cyberattacked entity brought by a damaged third party and costs associated with regulatory proceedings resulting from the cyberattack, including legal fees, fines, or sanctions.[13]

However, most cyber insurance polices exclude coverage for bodily injury or property damage. Because many commercial general liability policies exclude coverage for bodily injury and/or property damage resulting from electronic data loss, damage, or corruption, this can create a concerning gap in coverage for cyberattacks in the construction context. In addition, some cyber insurance policies make coverage contingent on the insured implementing and adhering to information security practices with which smaller entities may have difficulty complying.[14]

Coverage for cyberattacks may also be found under property/builder's risk policies, although this likely will depend on a fact-dependent and policy language-specific determination of whether damage to electronic data constitutes physical damage. Furthermore, criminal liability policies may cover certain cyberattacks, such as computer fraud.[15]

III. 3D-Printing

More formally known as additive manufacturing, 3D printing refers to "joining materials to make objects from 3D model data, usually layer upon layer, as opposed to substrative manufacturing methodologies." Although 3D printing has existing in the manufacturing industry for approximately 40 years, its use in the construction industry remains largely experimental.[16]

A. Potential Benefits

3D printing could offer potentially significant increased efficiency and decreased labor and material costs in the manufacture of construction components. With their relative swiftness in crafting complex shapes and ability to use a wide variety of materials (including recycled materials), 3D printers could offer substantial reduced costs for unique and complex construction components. Theoretically, 3D printing could be scaled to creating entire walls, foundations, or even whole buildings.[17]

B. Potential Risks/Liabilities

Because use of 3D Printing in the construction industry remains largely speculative, the precise legal ramifications of such use is uncertain. Areas of legal concern include: (a) potential

---

[13] *Id*.
[14] *Id*.; Patrick J. O'Connor, Jr., *Cyber Security and Cyber Insurance for the Design of Construction Industry*, 10 No. 1 ACCLJ 4 (Aug. 2016).
[15] Brennan, *supra* note 3.
[16] Vince Anawenter, et al., *Brave New Extruded World: Legal Issues Arising in the Construction Industry From Using Additive 3D Printing Technology*, 9 No. 1 ACCLJ 1 (Aug. 2015).
[17] *Id*.

application of the Uniform Commercial Code (UCC) to disputes over 3D-printed construction components; (b) approval by building code authorities; and (c) insurance coverage issues.[18]

1. Potential Application of the UCC

Although questions of the applicability of the UCC to construction projects are not new, 3D printing – with its inherent reduction and potential elimination of labor in creating construction components – would appear to increase the likelihood that a 3D-printed construction component or building would qualify as a "good" subject to the UCC rather than a "service" subject to traditional common law principles. This would impact numerous aspects of any dispute over 3D-printed materials, including: (a) accepting, rejecting, forming, and terminating the contract (b) imposing or disclaiming implied warranties; (c) creating express warranties; (d) imposing strict liability; (e) determining causation; (f) calculating damages; and (g) determining statute of limitations issues.[19]

2. Approval by Building Code Authorities

Current building codes assume the use of established construction design methods using standardized shapes and traditional construction materials. These codes provide little guidance for regulators in evaluating the structural adequacy of novel 3D-printed components and structures using extrudable materials, the long-term durability of which has yet to be established. Consequently, until new code provisions can be adopted based on proven metrics for evaluating the long-term structural adequacy of 3D-printable materials, code authorities may be reluctant to issue building permits for structures incorporating 3D-printed materials or components.[20]

3. *Insurance Coverage Issues*

As with current building codes, 3D printing does not fit well into typical commercial general liability or professional liability insurance coverages. Users of 3D-printing in the construction industry may need to either broaden their existing coverage or obtain separate products liability coverage. This may prove challenging, as insurers are likely to be cautious about insuring construction applications of 3D printing until they obtain a more thorough understanding of the risks involved.[21]

IV. Conclusion

Application of new automated and remotely operated technologies to the construction industry offers great potential for use and application on projects, including substantial increases in efficiency, coordination, and safety. However, they also introduce new risks and liabilities that

[18] *Id*.
[19] *Id*.
[20] *Id*.
[21] *Id*.

current risk management structures may not adequately address. Members of the construction industry, and their counsel, need to be aware of, understand, and address these risks in adopting and implementing such new technologies.