"Open the Pod Bay Doors HAL": Product Liability Implications of Product Innovations

July 8, 2019

2019 IADC Annual Meeting
Asheville, North Carolina

Presenters:

Stephen G.A. Myers, *Moderator*
Irwin Fritchie Urquhart & Moore, LLC
New Orleans, LA

Sylvie Gallage-Alwis
Signature Litigation AARPI
Paris, France

David L. Ferrera
Nutter McClennen & Fish LLP
Boston, MA

Richard J. Underwood
Exponent Inc.
Philadelphia, PA

Additional Contributors:

Annie Huang
Robins Kaplan LLP
New York, NY

Rayna E. Kessler
Robins Kaplan LLP
New York, NY

"Law lags science; it does not lead it." – Judge Richard Posner

Advances in technology give rise to new and complicated legal issues. These issues include how existing products liability and consumer protection laws will apply to Internet of Things products, products incorporating artificial intelligence and products manufactured by additives, or "3D Printing" technology. As discussed below, these product innovations will require product liability law to evolve and may raise a whole host of issues, such as insurance and intellectual property issues, risk assessment, jurisdictional issues, or legislative and regulatory issues. Section I of this paper addresses traditional principles of products liability law. Subsequent sections address product liability implications for products manufactured by 3D printing (II), products incorporating artificial intelligence (III), and Internet of Things products (IV).

I. Traditional Principles of Product Liability Law[1]

Products liability law developed to address individual who were injured by defects in (tangible)[2] products manufactured by a commercial[3] seller. The legal framework evolved at a time when product manufacturers tended to be large commercial enterprises, which were primarily responsible for the design and development of their products as well as their sale and distribution. This centralization of this activity supports an underlying premise of products-liability law that a "manufacturer" is most knowledgeable about the products that it sells and is in the best position to ensure that safe products reach the marketplace. Under such a paradigm, the imposition of strict liability theories on such manufacturers was deemed appropriate.

Mass production is the second characteristic of traditional manufacturing upon which products-liability law is based. Historically, products were uniform, mass-produced, and based upon a single (or small set of) design(s) as captured in the manufacturing specifications. Liability theories evolved out of this paradigm. For example, the Restatement (Third) of Torts describes theories of recovery based upon whether a product deviates from a manufacturing specification (manufacturing defect), whether the risks associated with the product's design specifications exceed the benefits (design defect), and whether the product (as designed) requires a specific warning to be used in a safe manner (inadequate warning).

[1] Sections I and II are authored by Stephen G.A. Myers and Richard J. Underwood.
[2] *See* Restatement (Third) of Torts: Prod. Liab. § 19(a).
[3] *See* Restatement (Third) of Torts: Prod. Liab. § 1 (indicating that to be subject to a products liability theory of recovery that a person or entity must be "engaged in the business of selling or otherwise distributing products." *But see id.*, at cmt. c. (providing that the liability does not apply to "noncommercial seller[s] or distributor[s]" nor to an "occasional or causal" sale).

II. Products Manufactured by 3D Printing

Additive manufacturing has the potential to unmoor traditional principles of strict liability described in Section I. The proliferation of 3D printing technology is likely to dispense with the historic, de facto requirement that a "manufacturer" be a large commercial entity that is also responsible for design and distribution activities. Likewise, the "mass production" paradigm will be replaced in time with the "mass customization" of products, given the lower costs and manufacturing flexibility that 3D-printing technology provides over traditional manufacturing.

A. What is Additive Manufacturing and How Does it Work?

Additive Manufacturing (AM), also known as 3D printing or rapid prototyping, is defined by ASTM International (formerly known as the American Society for Testing and Materials) as the "process of joining materials to make parts from 3D model data, usually layer upon layer, as opposed to traditional subtractive manufacturing and formative manufacturing methodologies."[4] The technology dates back to 1984, when Charles Hull, who later founded 3D Systems, Inc., patented a process described as "stereolithography" (solid imaging) using fluids and digital blueprints.

Additive manufacturing differs from the traditional manufacturing methods of subtractive manufacturing (e.g. milling, drilling or turning) and formative manufacturing (e.g. pressing, forging or stamping) as the part is "printed" in a machine from a digital model of the part layer by layer. The material that the part is manufactured from is built up, layer by layer, from the raw material by the printer, rather than starting the production process with a solid block of material which is cut and shaped to produce the final part.

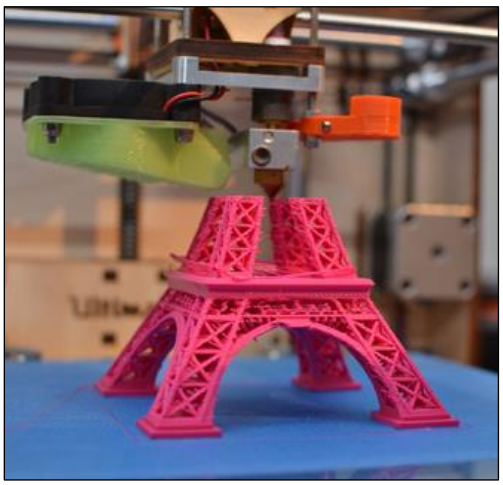


Figure 1 – Half-complete 3D printout of Eiffel Tower model

[4]ASTM International / The International Organization for Standardization, *52900:2015(E) Standard Terminology for Additive Manufacturing – General Principles – Terminology*, available at https://www.iso.org/obp/ui/#iso:std:iso-astm:52900:ed-1:v1:en.

The technology offers everybody the chance to become a "manufacturer," using either their own home 3D printer or one of many commercial entities offering 3D-printing services, such as UPS.[5] Parts can be printed from digital models created by the individual or from models downloaded from the internet. Some futurists predict that every house will soon have a 3D printer, displacing traditional factories and mass production entirely. Others have described the huge potential offered by this technology as "the next industrial revolution."

B. What Are the Benefits and Limitations?

There are many potential advantages to additive manufacturing. For example, it allows designers to produce easily customizable parts, or parts that cannot be manufactured by other production methods. Additionally, additive manufacturing has the potential to produce finished products, with multiple materials and moving pieces, and it allows production with no upfront cost due to manufacturing tooling. It also offers cost and time savings for prototype parts or smaller production runs. In terms of the potential, imagination is the limit!

Additive manufacturing does, however, have some disadvantages compared to traditional manufacturing methods. Currently, additive manufacturing processes may have slower build rates and are more expensive for mass production parts. Parts produced by additive manufacturing may have inferior or variable mechanical properties and are limited by the size of the available printer. Parts may require post-processing (cleaning, for example), further procedures to improve material properties, improvements to surface finish or further machining. Additionally, in some industries, the regulatory approval pathways are currently undefined.

C. Challenges of Additive Manufacturing

In some applications and industries, additive manufacturing offers significant advantages over traditional manufacturing processes. It is likely that the use of additive manufacturing techniques will only become more widespread in the future. However, additive manufacturing does come with a specific set of challenges and potential problems that do not exist with traditional manufacturing processes.

3D printers have hundreds of variables that may potentially affect the mechanical and geometrical properties of the finished part. While many of these variables are controlled by the printer software and established by the printer manufacturer, there are still many quality-critical factors under the control of the user.

---

[5] *See* The UPS Store, *3d Printing: Custom solutions to meet your unique business needs, Let your ideas take shape with 3D printing*, available at https://www.theupsstore.com/print/3d-printing.

D. Current Applications of Additive Manufacturing

1. Pharmaceuticals

In August 2015, the FDA approved the first 3D printed drug – Spritam, a drug used for treating epileptic seizures. The use of 3D printing allows the manufacturer to produce a tablet with a highly porous structure produced by the 3D printing, rapidly dissolves in the mouth with a sip of liquid. This allows a much larger dose of medication to be delivered in a form that will rapidly dissolve in the mouth compared to existing "fast melt" tablets.

In the future, researchers have speculated that it may be possible to "print your own medicine" on a home 3D printer. Using a printer loaded with a universal set of chemical inks, it may become possible to download a "chemical blue print" and carry out "on the fly molecular assembly." The proposed advantages include the ability to print drugs at the point of need or rapidly distribute a particular drug.

However, this also represents a significant departure from the traditional supply chain for pharmaceutical products. It also raises questions about whether the sale or license of an intangible, digital blueprint for a medicine would expose the designer or distributor of that blueprint to strict products liability. While not in the context of 3D-printed products, existing jurisprudence reflects a hesitancy of courts to label digital files, software, and/or intangible thoughts and ideas as "products" for purposes of products liability law. However, even the Restatement itself recognizes that there may be exceptions to the traditional requirement that "products" be tangible items. *See* Restatement (Third) of Torts: Prod. Liab. § 19(a) ("[o]ther items . . . are products when the context of their distribution and use is sufficiently analogous to the distribution and use of tangible personal property . . . ."). And this exception may ultimately swallow the rule if additive manufacturing results in this sort of supply-chain reconfiguration.

2. Medical Devices

The medical industry is also exploring the use of additive manufacturing technologies and can generally be separated into implantable and non-implantable devices and devices that are patient-matched or non-patient-matched.

a. Non-Implantable Products

Patient-matched devices are usually customized using either medical imaging data or laser scans of an individual patient's anatomy to modify the geometry of the resulting device. Patient-matched disposable custom cutting guides and drill templates are non-implantable products that are used by surgeons during arthroplasty procedures to aid the surgeon in positioning bone cuts and are derived by the manufacturer from computed tomography or magnetic resonance imaging scans of the patient. Their use can decrease surgical time, replace trays of reusable instruments, and are thought to reduce surgical errors during arthroplasty. However, opportunity for more widespread

use of such customized surgical aids (particularly when provided by a medical device manufacturer), also will increase the opportunities for plaintiffs' attorneys to argue that the manufacturer is now an active participant in the surgical procedure, a role traditionally limited to the surgeon and his or her surgical team. This is another example of how the adoption of additive manufacturing technologies could conceivably impact the scope of legal exposure for product manufacturers.

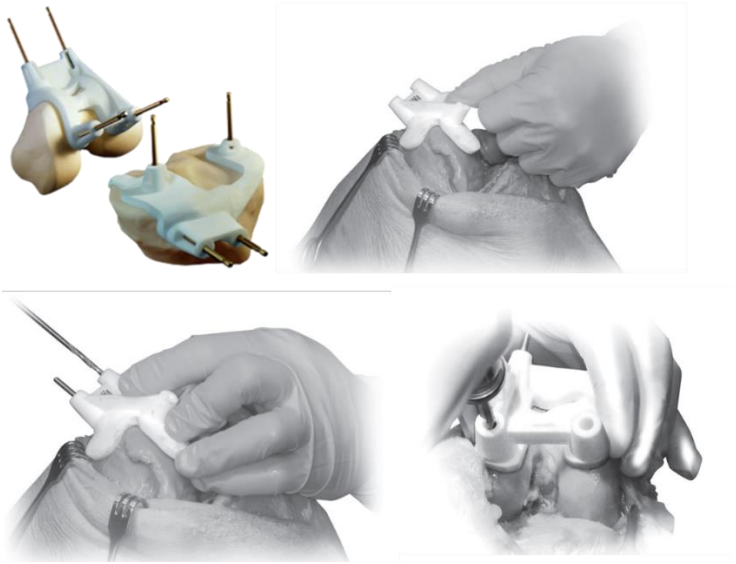


Figure 3 – Zimmer patient specific instrumentation[6]

b. Implantable Products

i. Standard-Sized Device Designs

Additive manufacturing is being used by device manufacturers to make standard-sized, or a range of discrete-sized, medical devices. The use of additive manufacturing allows manufacturers to make devices with features that would be either expensive or complex to manufacture using other methods.

An example of the use of additive manufacturing to manufacture standard-sized devices is the Zimmer Biomet Unite3D Bridge Fixation System, which is used in joint and ankle joint fusion surgery.[7] It is reported that the porous structure, "directly mimics

[6] *See* Zimmer, *Zimmer® PSI Knee Surgical Technique*, available at: http://www.zimmer.com/content/dam/zimmer-web/documents/en-US/pdf/surgical-techniques/knee/zimmer-psi-surgical-technique.pdf.

[7] Additive Manufacturing Today, *Zimmer Biomet Announces FDA Clearance for Metal 3D Printed Bridge Fixation System*, available at https://additivemanufacturingtoday.com/zimmer-biomet-announces-fda-clearance-for-metal-3d-printed-bridge-fixation-system.

the architecture of human cancellous bone."[8] Additive manufacture allows the solid and porous regions of the implant to be printed simultaneously.[9]

Figure 4 – Picture of Zimmer Biomet Unite3D™ Bridge Fixation System[10] and the structure of the porous structure of OsseoTi Porous Metal and human cancellous bone.[11]

ii. Patient-Matched Device Designs

Additive manufacturing also is being used in the manufacture of patient-matched devices. Patient-matched devices may be based on a standard template that can be modified to match the patient's anatomy either by scaling the device, matching to specific anatomical landmarks or using a model of the patient-specific anatomy from imaging. The design of a patient-specific device may be carried out either by clinical staff, the device manufacturer or a third party.

An example of the trend to mass customization can be found in total knee replacements. ConforMIS currently offers patient-matched orthopaedic implants based on medical imaging data.[12] In this process, a CT scan of the knee is converted to a 3D model by

---

[8] Zimmer Biomet, *OsseoTi® Porous Metal Technology*, available at http://www.zimmerbiomet.com/medical-professionals/foot-and-ankle/product/osseoti-porous-metal.html.

[9] 3Printer, *Zimmer Biomet Receives FDA Clearance for 3D Printed Unite3D Ankle Fusion Systems*, available at https://www.3printr.com/zimmer-biomet-receives-fda-clearance-for-3d-printed-unite3d-ankle-fusion-systems-3335468/.

[10] Additive Manufacturing Today, *Zimmer Biomet Announces FDA Clearance for Metal 3D Printed Bridge Fixation System*, available at https://additivemanufacturingtoday.com/zimmer-biomet-announces-fda-clearance-for-metal-3d-printed-bridge-fixation-system.

[11] Gautam Gupta, Ph. D., *OsseoTi Porous Metal for Enhanced Bone Integration* an Animal Study, available at http://www.zimmerbiomet.com/content/dam/zimmer-biomet/medical-professionals/foot-and-ankle/osseoti-porous-metal/osseoti-porous-metal-for-enhanced-bone-integration-an-animal-study.pdf.

[12] *See* ConforMIS, *Total Knee Replacement,* available at http://www.conformis.com.

mapping the articular surface of the joint. Additive manufacturing technology then is used to form an implant from cobalt-chromium alloy based on a patient's own CT scan.[13,14]

Figure 5 – iTotal kit of pre-sterilized and disposable custom instruments and ConforMIS knee components[15]

E. Legal Implications

Mass customization of medical implants raises a host of unanswered legal queries. As mentioned, products-liability law is predicated on a mass-production environment. In that setting, manufacturing specifications typically are uniform, and thus, it is relatively straightforward to evaluate whether a product complies with its manufacturing specifications in the context of a manufacturing-defect claim. Likewise, a risk/benefit analysis of an overarching design (as defined by product specifications) is possible among a broad population of users to determine whether a particular design is

---

[13] Although each implant is matched to an individual patient, this device was cleared for use under the 510(k) regulatory pathway. US Food and Drug Administration (FDA) has indicated that patient-matched medical devices are not considered to be "custom" devices as defined by section 520(b)(2)(B) of the FD&C Act and therefore do not qualify for a custom device exemption from premarket notification. *See* M. Di Prima, J. Coburn, D. Hwang, J. Kelly, A. Khairuzzaman, L. Ricles, *Additively manufactured medical products – the FDA perspective*, 3D PRINTING IN MEDICINE, 2 (2016) 1-6.

[14] As stated in the draft FDA guidance *(see Appendix B)*, "Patient-specific devices are, in general, ones in which ranges of different specifications have been approved or cleared to treat patient populations that can be studied clinically. Premarket submissions for such devices are sometimes referred to as 'envelope' submissions because their approval or clearance covers the entire range of specifications data they contain to support. The final manufacturing of these devices can be delayed until physicians provide imaging data or other information to the manufacturer to finalize device specifications within cleared or approved ranges. As a result, such devices are specifically tailored to patients." *See* M. Di Prima, J. Coburn, D. Hwang, J. Kelly, A. Khairuzzaman, L. Ricles, *Additively manufactured medical products – the FDA perspective*, 3D PRINTING IN MEDICINE, 2 (2016) 1-6.

[15] *See* Scott J Grunewald, *3D Printed Knee Replacement Manufacturer ConforMIS (CFMS) Raises $135M As The Company Goes Public*, available at https://3dprint.com/78272/conformis-3d-printed-knee/.

"defective." But this sort of legal inquiry is complicated in the context of customized products.

For example, if a person that has received a customized implant ultimately requires a revision procedure, the implant manufacturer could face significant challenges if a design defect claim is asserted. The alternative-design/risk-utility test employed in most jurisdictions becomes weighted in the plaintiff's favor because:

(1) There are an infinite number of alterative designs available to the manufacturer using 3D printing technology;

(2) There is a reduced feasibility hurdle that weighs against the alternative design (because all designs may be possible to print using additive manufacturing);

(3) There is not a broader population of implant recipients available to demonstrate the principle that widespread benefits of the implant outweigh the particular risks that occurred for the plaintiff.

Moreover, Plaintiffs' lawyers will surely argue that the manufacturer failed to appropriately test their customized products. But it is impossible, practically speaking, for a manufacturer to test each of the theoretically unlimited product designs that are now available via additive manufacturing in the same manner in which a single design traditionally would have been tested during research and development.

Europe also is grappling with the legal implications of 3D-Printed products.[16] In June 2018, the European Union Parliament has asked to the European Union Commission to work on a number of issues relating to 3D printing and liability. The issues raised by the Parliament show clearly what legal issues may be discussed in the scope of litigation. The Parliament indeed:

- "*Calls on the Commission to carefully consider the civil liability issues related to 3D-printing technology, including when it assesses the functioning of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products;*
- *Calls on the Commission to explore the possibility of setting up a civil liability regime for damages not covered by Directive 85/374/EEC;*
- *Points out that 3D-printing technology has many economic advantages for the EU as it offers opportunities for customisation specifically meeting the requirements of European consumers, and that it could make it possible to repatriate production activities and thereby help to create new jobs that are less physically demanding and less dangerous;*
- *Calls on the Commission to clearly define the various responsibilities by identifying the parties involved in making a 3D object: software designer and supplier, 3D printer*

[16] European implications authored by Sylvie Gallage-Alwis.

manufacturer, raw materials supplier, object printer and all others involved in making the object;
- *Draws attention to the possible implications of new forms of marketing along the lines of 'make it yourself', supplying not the final product but only the software for download and the specifications for printing the product;*
- *Stresses the importance of creating a coherent legal framework to provide a smooth transition and legal certainty for consumers and businesses in order to promote innovation in the EU*"[17]

F. Conclusions

In theory, 3D printing has the potential to reduce an entire manufacturing facility into a single 3D printer that might range in size from a desk to a desktop. "Manufacturing" then becomes as easy as hitting a button from within computer-aided-design (CAD) software once the product has been digitally designed.

Ultimately, two aspects of additive manufacturing are likely to have the most significant impact on products-liability law: (1) the mass customization of products; and (2) the inevitable dissociation of product design, manufacturing, and sales.

As previously noted, products-liability law was formulated to address injuries to individuals resulting from mass-produced products. As such, the products-liability law framework that developed does not immediately lend itself to the analysis of injuries from custom-made items. Moreover, the fracture or dissociation of product design, manufacturing, and sales, which is now more likely with the adoption of additive manufacturing, will require a reanalysis of fundamental products-liability questions, such as: what is a product? (e.g., tangible item or digital model) and who is a manufacturer? (e.g., designer of digital model or owner of 3D printer that prints the item).

Unfortunately, the law lags technology, and the preceding issues have yet to be addressed by our courts. Our research reveals only one decision addressing liability for a 3D-printed product, the Invisalign orthodontic system. But the case focused on allegations of misrepresentations regarding the effectiveness of the system, as opposed to more product-oriented allegations of the sort that we have raised here.[18]

Thus, while there is dearth of legal authority on the subject, there are nonetheless common-sense steps that corporate manufacturers and their outside legal counsel should keep in mind when venturing into these untested waters:

1. Consider the potential ramifications of new business ventures employing additive manufacturing and evaluate whether the new

[17] Committee on Legal Affairs of the European Union Parliament, on three-dimensional printing, a challenge in the fields of intellectual property rights and civil liability (2017/2007(INI)).
[18] *See Buckley v. Align Technology, Inc.*, No. 5:13-CV-02812-EJD, 2015 WL 5698751, (N.D. Cal. Sept. 29, 2015).

venture could subject the company to a new type of exposure, such as strict product liability.

2. Reevaluate hold-harmless and indemnity agreements with vendors and component-part suppliers when additive manufacturing is being used by any entity in the supply chain.

3. Examine all types of corporate insurance to determine whether additive manufacturing is the subject of any exclusions or special treatment.

4. Ensure that company employees and engineers are monitoring regulatory and trade organization activities on the subject – and updating company practices and protocols accordingly.

Additive manufacturing technology is exciting and likely to have an impact on industry and the associated legal landscape, but corporate manufacturers should monitor developments closely to ensure that potential legal implications are understood and exposure is minimized.

III. Products Incorporating Artificial Intelligence[19]

The rise of artificial intelligence ("AI") technologies in the diagnosis and treatment of patients also challenge traditional notions of product liability law.

For example, the UK National Health Service (NHS) operates a telemedicine number called "NHS 111" that provides clinical assessments as part of the NHS urgent care system. To ease pressure on the telephone system, NHS England plans to move 30% of NHS 111 callers over to apps and websites, and to use AI and machine learning to answer patient questions like "Is the pain getting better? Yes or no." leading to related questions and an ultimate conclusion. Questions remain regarding publication of peer review clinical data to support the claim that the system is 100% safe – and whether in fact it results in significant cost savings.

Surgical robots provide a more extreme example. Although robots have been assisting surgeons for years in the form of advanced surgical instruments, medical innovation is on the cusp of a new development that would remove the surgeon from the operating room entirely: autonomous robotic surgery (ARS).

As more medical device manufacturers offer AI technologies like ARS to their surgeon customers, traditional lines of legal defense most often taken by companies may change.

[19] The section is authored by David L. Ferrera.

A. What Will Be Required To Be Communicated to Patients?

Traditional product liability law holds that doctors are uniquely suited to advise their patients of the risks and benefits of a course of medical treatment, taking into account the patients' individual medical history and future needs. Given the medical complexities involved, medical device manufacturers typically are not expected to warn patients directly about surgical risks and benefits. Instead, the surgeon stands between the medical device manufacturer and the patient as a "learned intermediary" responsible for providing adequate warnings, because the surgeon has unique knowledge of the patient's treatment options and the associated risks and benefits given current surgical practice. ASR would largely remove the surgeon from this traditional equation, thus eliminating the learned intermediary. Without the surgeon, then, the question is whether companies who manufacture the robots will be responsible for communicating risks and benefits directly to patients.

ASR should not shift the existing legal landscape this dramatically. Although surgeons may be physically removed from the operating room, they will not be removed from the decision-making process. Surgeons will continue to play an important role in recommending ARS, explaining the pros and cons, and discussing alternative options. As the medical professionals responsible for helping patients decide whether to undergo ARS, a surgeon should still be viewed as a learned intermediary, and ASR manufacturers should continue to receive this valuable defense in product liability litigation.

B. What Will Be the FDA Regulatory Pathway to Market?

There are two regulatory pathways for medical devices to come to market following U.S. FDA review: so-called "510(k) clearance" for devices "substantially equivalent" to those already on the market, and "pre-market approval" for more innovative devices. Under traditional product liability law, medical devices that undergo pre-market approval obtain protection from many state law legal claims under a doctrine called "federal preemption." In essence, preemption holds that a lay jury may not second-guess the safety assessments of FDA professionals. Although robotic-assisted surgery is not new, ARS is a significant technological advancement, likely to involve more complex hardware and software. Thus, autonomous robots should be subject to the FDA's pre-market approval process, rather than 510(k) clearance. If that is the case, state law claims against manufacturers of FDA-approved ARS systems for defective design or inadequate warnings should remain ripe for early dismissal as preempted by federal law.

C. What is the "Product"?

Because only "products" are subject to strict liability causes of action, defining the "product" is a key part of determining exposure to liability. Surgical robots are unique in that they require both hardware and software to operate. While hardware is certainly

a "product," most courts do not consider software to be a "product." But, in 2016, the FDA issued draft guidance stating that software is a "medical device" subject to FDA regulation. Although this guidance is not legally binding, it echoes the holdings of some courts that software is a "product."

The debate about what components of ARS constitute "products" is not academic. Rather, it highlights an inevitable issue that manufacturers will face in defending against lawsuits: was the patient's injury caused by a defect in the robot or in the software that powers it? If different manufacturers collaborated to create the final ARS system, this issue could lead to finger pointing if the co-defendant manufacturers do not collaborate to present a unified front at the outset of a litigation.

D. FDA's Position on AI/ML-Based SaMD

On April 2, 2019, FDA published an exploratory white paper proposing a new regulatory framework for medical devices containing AI or machine learning based software.[20] Stakeholders may comment on the discussion paper through June 3, 2019. FDA also launched a new webpage titled "Artificial Intelligence and Machine Learning in Software as a Medical Device."[21]

FDA's white paper acknowledges a difficulty found with AI products; namely, algorithms that continually adapt based on new data are not well suited to the current regulatory scheme. Traditionally, software was "locked" at design, providing the same output to a particular input, and requiring manual modification to incorporate learning or updates. AI introduces "adaptive" or continuously learning algorithms, such that the outputs may be different after changes are implemented by machine learning following analysis of a particular set of inputs. FDA proposes a "Total Product Life Cycle" approach to modifications of AI/ML-based software as a medical device. The agency identifies four general principles to balance benefits and risk, including new ideas about (1) establishment of clear expectations on quality systems and good machine learning practices; (2) premarket review for reasonable assurance of safety and effectiveness, potentially leveraging more the "de novo" review pathway; (3) monitoring of algorithm changes; and (4) monitoring of post-market real-world performance.

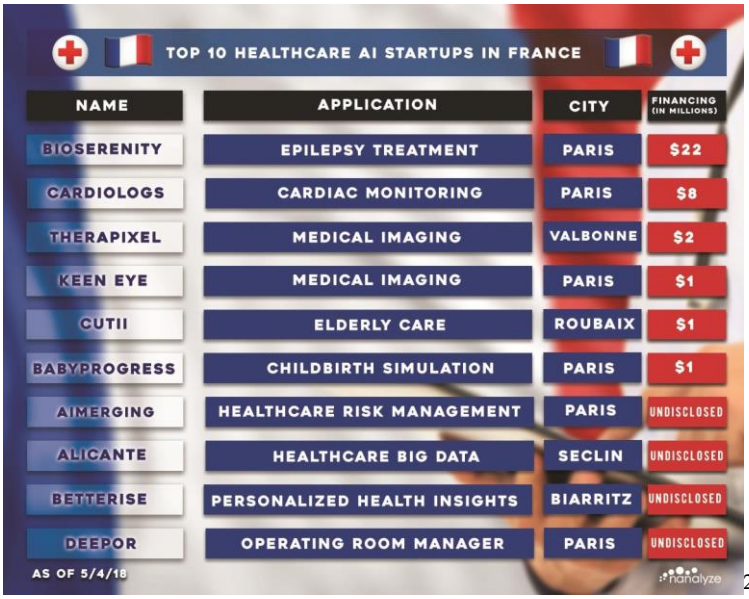
Some commentators have described the FDA's problem of AI oversight as trying to hit a moving target while regulating it. Comments to the proposed white paper may address concerns about the proposed regulatory framework's effects on preemption and the duty to warn/learned intermediary doctrine. Ultimately, courts may decide that a fact-based inquiry is necessary to determine whether FDA's up-front review and continuous

[20] The white paper can be found at https://www.regulations.gov/document?D=FDA-2019-N-1185-0001.
[21] The web page can be found at https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device.

monitoring of algorithm changes are rigorous enough to provide traditional legal protections to manufacturers.

E. The European Position[22]

Medical devices and AI are a prominent topic in the EU as well. Many startups have been created for this purpose. France is one of the leading countries in this respect as shown by the below summary.



[23]

What is worth noting is that none of these startups have been created by experts in medical devices but rather by experts in AI. This has led to numerous questions on future liability and the role the health industry should play.

The High Health Authority (HAS – *Haute Autorité de la Santé*) has published guidelines in February 2019 on how clinical trials on medical devices containing AI should be conducted. Apart from the warning that manufacturers should be the ones which be held liable according to the HAS, the latter warns against data privacy issues and its power to alert data privacy protection authorities around the world should sensitive data, such as medical data, be misused.

On December 7, 2018, the European Commission and the Member States published a Coordinated action plan on the development of AI in the EU *"in order to promote the development of artificial intelligence (AI) in Europe*"[24].

[22] This section authored by Sylvie Gallage-Alwis.
[23] Source: https://www.nanalyze.com/2018/05/10-french-startups-ai-healthcare/
[24] See: https://ec.europa.eu/digital-single-market/en/artificial-intelligence

IV. Internet of Things Products[25]

In our ever-more connected world, the Internet of Things ("IoT") refers to a variety of internet-connected devices from light bulbs to smart appliances to wearable fitness trackers. Through embedded sensors, these IoT devices collect information such as audio, video, biometric or geolocation data. The collected information is stored in data centers that allow analytic engines to provide feedback or control. IoT products tout many benefits to consumers, including many products that offer convenience, safety and health benefits. For example, IoT medical devices can track a patient's health data to assist with the patient's diagnosis and treatment. The rapid proliferation of IoT products has been stunning. Gartner, a technology research company, estimated that there were 8.4 billion IoT devices in use in 2017—a 31% increase since 2016.[26] The growth continues as Business Insider estimates that about 55 billion IoT devices will be installed around the world by 2025.[27] A significant portion of these IoT devices is expected to be health-related.

Under traditional principles of strict liability described in Section I, fault flows up the chain of distribution from the retailer through distributors, and ultimately to the manufacturers. The policy rationale is that manufacturers are in the best position to prevent harm from product defects.[28] With IoT products, there is an additional layer of software developers—are they liable in the event the software is vulnerable to an outside attack? Within the three primary categories of product defect liability—manufacturing defects, design defects, and defective or inadequate warnings[29]—"software defects have typically been seen as design defects, though in some cases harm could be caused by a 'random failing or imperfection' in a software product, and thus be deemed a manufacturing defect."[30] Courts, however, are split on the question of what standard to apply to design defect cases.[31] Consumers add yet another layer as they may also be apportioned fault if a consumer failed to properly secure the IoT device by using an easily hacked password, downloading malware, or failing to update security software.

---

[25] The section is authored by Annie Huang and Rayna E. Kessler.
[26] *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 percent from 2016*, Gartner (Feb. 7, 2017), https://www.gartner.com/newsroom/id/3598917.
[27] Peter Newman, *IoT Report: How Internet of Things The Internet of Things technology is now reaching mainstream companies and consumers,* Business Insider (Jul. 27, 2018), https://www.businessinsider.com/internet-of-things-report.
[28] Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused By Hacked Devices?*, 50 U. Mich. J.L. Reform 913, 916 (2017).
[29] *See* Restatement (Third) of Torts: Prod. Liab. § 2.
[30] Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused By Hacked Devices?*, 50 U. Mich. J.L. Reform 913, 917 (2017).
[31] *See, e.g., Tincher v. Omega Flex, Inc.*, 104 A.3d 328 (Pa. 2014) (attempting to resolve the common law test for design defects in Pennsylvania based on conflicting interpretations in the Second Restatement, the Third Restatement, and prior case law).

The application of IoT in the healthcare industry is used below to explore its impact on products liability and other related issues.

A. Application of IoT in the Healthcare Industry

IoT touches upon nearly every segment of the healthcare industry. IoT medical devices and applications have helped deliver enhanced diagnostics, improved doctor-patient communications, and better diagnostics and treatment of patients. Some of the most significant benefits of IoT medical products can be found outside of hospitals in the following categories.[32]

- *Remote monitoring*: constant connection from patient to caregiver from anywhere in the world. For example, diabetics require constant monitoring of their glucose levels. Remote monitoring connects glucose readings to a smartphone, then to a physician who can modulate the patient's care in the closed ecosystem.
- *Telemedicine*: reduces the need for making physical office visits for less critical for routine appointments.
- *Behavioral modification*: offers "life coach in your pocket" on how to manage certain health characteristics such as eating the proper diet and reminders to take medication.

Examples of connected health and medical devices include pacemakers, insulin pumps, hearing aids, glucose monitors, heart rate patches and wireless scales for monitoring congestive heart failure, sensors in shoes to detect falls and gaits, patient identification and tracking, and baby monitors with temperature, heart rate, and other sensors.

B. Cybersecurity Risks and Privacy Threats

IoT presents many cybersecurity risks and threats to privacy. In 2015, the healthcare industry was the most cyberattacked industry.[33] Even if cyberattacks are not deliberately targeting medical devices, if these devices are connected to a hospital network, they may be impacted.[34] Recent data breaches highlight the difficulty organizations face in trying to protect personal data.[35]

---

[32] *Mobile Medicine: The Internet of Things Meets Health*, Goldman Sachs, https://www.goldmansachs.com/insights/pages/iot-meets-health.html.
[33] Zlata Radionova, *Healthcare is now top industry for cyberattacks, says IBM*, Independent (Apr. 21, 2016), https://www.independent.co.uk/news/business/news/healthcare-is-now-top-industry-for-cyberattacks-says-ibm-a6994526.html.
[34] *Statement from FDA Commissioner Scott Gottlieb, M.D., on FDA's efforts to strengthen the agency's medical device cybersecurity program as part of its mission to protect patients* (Oct. 1, 2018), https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm622074.htm.
[35] *The biggest healthcare data breaches of 2018 (so far)*, Healthcare IT News, as of Oct. 25, 2018, https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far.

Issues associated with networked medical devices include:

- Untested, unpatched, or defective software and firmware
- Theft or loss of networked medical devices (external or portable)
- Lack of standards
- Unauthorized device setting changes, reprogramming, or infection via malware
- Denial-of-service attacks
- Targeting mobile health devices using wireless technology to access patient data, monitoring systems, and implanted medical devices.

The following example illustrates the potential uses and challenges of IoT:

> a connected health (or a smart health) application for smart phones and watches called Fido that is designed by a company named Fjord. While current non-IoT devices can detect one's glucose level at a point in time and recommend an appropriate insulin dose, Fido promises several functionalities to better manage the chronic diabetic condition. First, Fido is device-agnostic. That is, it will work on many devices such as smartphones and watches. Second, it measures and records not just glucose level but also nutrition, stress level, sleep, and activity, and does so either automatically or through consumer input. It also measures all of this data over long periods of time. This collection of a variety of data at a granular level via various sensors speaks to the enormous scale of IoT data over what computers can currently collect. Third, by aggregating data from several people, it can discern the pattern between glucose level and various consumer habits, and thus, suggest behavioral changes to help manage that glucose level. This would not be possible without enhanced data analytics capabilities. Fourth, when a consumer's glucose level goes over a safe threshold, Fido can alert healthcare providers to enable a timely, life-saving intervention.[36]

In this example, Fido shows the potential benefits of IoT, but also presents a reminder of IoT's privacy and security implications. Health data is sensitive, and its granularity presents significant challenges to anonymizing personal information, which exposing consumers to privacy and data security risks.[37]

C. Additional Risks

In addition to cybersecurity risks, IoT devices in the healthcare field face other unique risks, two of which are discussed below. With devices that monitor vital signs, there is the risk of overdiagnosis, which occurs when there is an accurate detection of

---

[36] Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 Berkeley Tech. L.J. 997, 998-99 (2016).
[37] *Id.*

deviations or abnormalities that are "not clinically important."[38] The following example regarding an infant physiologic monitor illustrates this risk.

> By continuously monitoring healthy infants, parents will inevitability experience some alarms for conditions that are not life-threatening, including false positives alarms due to motion artifact or other causes, and true positive alarms for events that are not clinically important. It is well-established that healthy infants have occasional oxygen desaturations to below 80% without consequence, placing them at risk of overdiagnosis and harm if these innocuous events generate alarms…a single abnormal test—such as a self-resolving desaturation—can trigger a cascade of events…prompt[ing] an emergency department visit with blood tests, x-rays, and hospital admission. Rather than reassuring parents, these experiences may generate anxiety and a false assumption that their infant is at risk of dying.[39]

Thus, rather than being life-saving, there is the potential that devices that monitor vital signs could result in harming the infant.

Whether there is sufficient battery power can pose another risk for manufacturers of IoT medical devices. Having a device shutdown and interrupt treatment can result in serious patient injury or death. In addition to device shutdown, there are other issues that can lead to patient harm such as the battery charge indicator not functioning properly, failing to show the correct status of the battery charge, or the battery depleting sooner than expected. In fact, on November 1, 2018, the FDA issued a letter to health care providers warning of a device failure for an intra-aortic balloon pump shutting down while running on battery power.[40]

With risk comes fear of injury or an actual injury, which means litigation and regulatory investigations may follow. The next section addresses some recent litigation involving IoT devices followed by regulatory and legislative guidance that will be important to monitor as they will likely impact the development product liability law concerning IoT devices.

---

[38] Christopher P. Bonafide, MD, MSCE, David T. Jamison, MA, BSEE, PMP, and Elizabeth E. Foglia, MD, MSCE, *The Emerging Market of Smartphone-Integrated Infant Physiologic Monitors*, Journal of the American Medical Association (Jan. 24, 2017).

[39] *Id*.

[40] *Device Failure Associated with Getinge's Maquet/Datascope Intra-Aortic Balloon Pumps-Letter to Health Care Providers*, FDA (Nov. 1, 2018), https://www.fda.gov/MedicalDevices/Safety/LetterstoHealthCareProviders/ucm624734.htm?utm_campaign=Device%20Failure%20Associated%20with%20Getinge%27s%20Maquet%2FDatascope%20Intra-Aortic%20Balloon%20Pumps&utm_medium=email&utm_source=Eloqua

D. Recent Litigation Involving IoT Products

Case law concerning IoT devices is still developing, especially with respect to medical devices, but litigation involving other types of IoT devices may be instructive. Cases concerning IoT products have generally focused on the threshold issue of standing and whether enough harm has been alleged by plaintiffs. In a matter involving certain Chrysler vehicles, the plaintiffs alleged that a security flaw in the vehicles' infotainment center turned the "vehicles into rolling deathtraps: the uConnect system has design vulnerabilities that allow hackers to take remote control of the vehicle's functions, including the vehicle's steering and brakes, to comical or disastrous effect."[41] The plaintiffs filed a class complaint seeking monetary damages and injunctive relief for fraud, negligence, and breach of warranty violation.[42] The defendants filed a motion to dismiss based on the speculative nature of the damages claim and "complain[ed] the loudest about standing."[43] The court found that plaintiff lacked standing to pursue damages for a risk of harm or a fear of that risk, but found standing to pursue damages for the diminished value of the vehicle because "the ongoing vulnerabilities have reduced the market value of their vehicles."[44] The case is still pending. Earlier this summer, the court granted certification of several state classes.[45]

In *Ross v. St. Jude Medical Inc.*, the plaintiff filed a proposed class action alleging the cardiac devices at issue contained remote monitoring technology that lacked the "most basic security defenses (such as strong authentication, encrypted software and code, anti-debugging tools, anti-tampering mechanisms and the use of a wand to activate RF wireless communications) that are used by other cardiac device manufacturers."[46] The plaintiff did not suffer any physical harm, but alleged that the cardiac devices were vulnerable to a "'crash attack' that would remotely disable the implanted cardiac devices" as well as a "'battery drain attack' that remotely runs down the batteries of the cardiac devices."[47] The plaintiff also alleged that it defendant owed patients a "duty of care" to ensure that devices safeguarded against potential hacking.[48] Four months after filing suit, the plaintiff voluntarily dismissed the lawsuit without prejudice.

The *In re VTech Data Breach Litigation* arose because a hacker bypassed VTech's security measures and obtained the personal data of millions of VTech's customers including parents' names, email addresses, and account password information as well as

---

[41] *Flynn v. FCA USA LLC*, No. 15-cv-0855-MJR-DGW, 2016 U.S. Dist. LEXIS 130614, at *2-3 (S.D. Ill. Sep. 23, 2016).
[42] *Id.* at *3-4.
[43] *Id.* at *5.
[44] *Id.* at *12-13, 35-36.
[45] *Flynn v. FCA USA LLC*, No. 15-cv-0855-MJR-DGW, 2018 U.S. Dist. LEXIS 111963, at *41-44 (S.D. Ill. Jul. 5 2018).
[46] *Ross v. St. Jude Medical Inc.*, Case No. 2:16-cv-06465 (C.D. Cal. Aug. 26, 2016), Complaint ¶ 27.
[47] *Id.* ¶ 29.
[48] *Id.* ¶ 76.

children's names, genders, birthdates and photos.[49] The hacker provided the data to a journalist and was arrested shortly thereafter.[50] The plaintiffs alleged an increased risk of harm and diminished value of the products and asserted claims for breach of contract, breach of warranty of merchantability and violations of state consumer protection laws. [51] VTech moved to dismiss the complaint for lack of standing and also argued that plaintiff had not suffered actual injury because the data was never used to perpetrate identify theft. The court dismissed the complaint without prejudice for failure to state a claim, but found that plaintiffs had standing with respect to their allegations of diminished value of their VTech products.[52] Plaintiffs amended their complaint, but the court again dismissed several claims and allowed plaintiffs to amend others.[53] A few months later, the parties settled the litigation.[54]

The VTech hack also prompted regulatory scrutiny. The Federal Trade Commission charged that VTech violated the Children's Online Privacy Protection Act by failing to establish and follow adequate data security practices.[55] The FTC also alleged that VTech violated the FTC Act by falsely stating that in its privacy policy that most personal data submitted by users would be encrypted, but VTech never encrypted any collected data.[56] VTech settled with the FTC in January 2018. The settlement required VTech to pay a $650,000 penalty and implement a comprehensive data security program that will be subject to independent biennial audits for 20 years.[57] The settlement marked the FTC's first children's privacy and security case involving internet-connected toys.[58]

E. Regulatory Guidance

In October 2018, the FDA announced efforts to strengthen the agency's medical device cybersecurity program.[59] The announcement reaffirmed the FDA's commitment to "proactively address medical device cybersecurity [a]s a key priority."[60] This was also in follow-up to the FDA's Medical Device Safety Action Plan[61] announced in April 2018, which includes the advancement of medical device cybersecurity.

---

[49] *In re VTech Data Breach Litigation*, Case No. 15-cv-10889-MSS, Docket No. 109 at 3 (Apr. 18, 2018).
[50] *In re VTech Data Breach Litigation*, Case No. 15-cv-10889-MSS, Docket No. 87 at 5 (Jul. 7, 2017).
[51] *Id.* at 6-7.
[52] *Id.* at 11-12, 27.
[53] *In re VTech Data Breach Litigation*, Case No. 15-cv-10889-MSS, Docket No. 109 at 23 (Apr. 18, 2018).
[54] *In re VTech Data Breach Litigation*, Case No. 15-cv-10889-MSS, Docket No. 117 (Sep. 12, 2018)
[55] *Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC* (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm622074.htm.
[60] https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm622074.htm.
[61]https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM604690.pdf.

The FDA's efforts began on October 1, 2018 with the launch of a preparedness and response "playbook" for healthcare delivery organizations to address threats to medical device cybersecurity.[62] The playbook was developed with MITRE to advise healthcare organizations on securing their medical equipment.

On October 16, 2018, the FDA announced a new agreement[63] with the US Department of Homeland Security (DHS) that aims to improve coordination and cooperation between the two agencies on medical device cybersecurity.

On October 18, 2018, the FDA issued "Content for Premarket Submissions for Management of Cybersecurity in Medical Devices,"[64] as an update to the original 2014 guidance with revised recommendations. The new recommendations include the cybersecurity bill of materials, a list of the software and hardware components of a medical device that may be vulnerable to cyber threats. A comment period is currently open through March 18, 2019.

In the Draft Guidance, the FDA focuses on cybersecurity recommendations in the following areas: device design, labeling and documentation. The scope of the Draft Guidance is broad, covering premarket submissions that contain software, programmable logic, and software that is considered a medical device, including Premarket Notifications (i.e. 510ks), de Novo requests, PMAs, Product Development Protocols, and Humanitarian Device Exemption applications.

Previously in 2016, the FDA issued the final guidance for "Postmarket Management of Cybersecurity in Medical Devices,"[65] which informed manufacturers of the Agency's recommendations for management of postmarket cybersecurity vulnerabilities for marketed and distributed medical devices once they are distributed to patients.

Currently, the FDA is proposing in the FDA's Fiscal Year 2019 Budget to create a Center of Excellence for Digital Health.[66] This center "would help establish more efficient regulatory paradigms, consider the building of a new capacity to evaluate and recognize third-party certifiers, and support a cybersecurity unit to complement the advances in software-based devices."

---

[62] https://www.mitre.org/publications/technical-papers/medical-device-cybersecurity-regional-incident-preparedness-and.

[63]https://www.fda.gov/AboutFDA/PartnershipsCollaborations/MemorandaofUnderstandingMOUs/DomesticMOUs/ucm623568.htm.

[64]https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf.

[65]https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf.

[66] https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm622074.htm.

F. Forthcoming Legislative Guidance

In October 2017, Congress introduced in the U.S. House of Representatives the Internet of Medical Things Resilience Partnership Act of 2017. The legislation's purpose is to "establish a working group of public and private entities led by the Food and Drug Administration to recommend voluntary frameworks and guidelines to increase the security and resilience of Internet of Medical Things devices, and for other purposes." The proposed working group is led by the FDA and include the FTC, the U.S. Departments of Health and Human Services and Commerce, the National Institute of Standards and Technology, the National Cyber Security Alliance, as well as representatives from medical device manufacturers, wireless network providers, enterprise security solutions systems, cloud-computing experts, healthcare providers and insurers, web-based mobile application developers, and software and hardware developers.

This working group is responsible for generating a report recommending voluntary frameworks and guidelines to increase security and resilience of Internet of Medical Things devices, focusing on:

(1) identifying existing cybersecurity standards, guidelines, frameworks, and best practices that are applicable to mitigate vulnerabilities in medical devices;

(2) identifying existing and developing international and domestic cybersecurity standards that mitigate vulnerabilities in such devices;

(3) identifying high-priority gaps for which new or revised standards are needed; and

(4) creating potential action plans by which gaps can be addressed.[67]

This group is required to submit its report by April 2019.

G. The EU – Still at Debating Time[68]

While issues and even litigation are fast evolving in the US, the EU is still debating as to how to approach IoT and more generally robots-related litigation and what should be the legal regime.

The European Parliament first adopted, on February 16, 2017, a resolution with "recommendations to the Commission on Civil Law Rules on Robotics." In this resolution, the Parliament expressly requests that the Commission submit a proposal for a directive on civil law rules on robotics, including the creation of "a specific legal

[67] H.R.3985 – Internet of Medical Things Resilience Partnership Act of 2017, 115th Congress (2017-2018), introduced in House on Oct. 5, 2017.
[68] This section authored by Sylvie Gallage-Alwis.

status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of [responsible] electronic persons." The European Parliament has thus decided to encourage a significant overhaul of the applicable laws in European countries and enable the creation of a "robotic personality".

Furthermore, the Parliament is urging the Commission to adopt a common European definition of the different categories of robots, to create a robot registration system for traceability purposes and a dedicated European agency. A "Charter on Robotics" is also mentioned to lay down the basic "ethical principles to be respected in the development […] of robots." The European Parliament defends the idea that the question of "intelligent and autonomous robots" has to be settled at a European level so as to "ensure the same degree of efficiency, transparency and consistency in the implementation of legal certainty throughout the European Union for the benefit of citizens, consumers and businesses alike".

If the EU decides to sanction the principle of a "robotic personality", this new status will have to be defined with a complete set of rules. In such a case, robots would enjoy rights and have obligations; they could also perform a certain number of legal acts depending on their level of autonomy. As discussed above, it is difficult to separate the concept of personality from the concept of liability; robot liability also has to be defined. However, the resolution provides that "at least at the present stage the responsibility must lie with a human and not a robot." The European Parliament, in its resolution, calls on the Commission to "establish a compulsory insurance scheme" for owners of autonomous robots to be able to compensate victims in the event of damage caused by their robot. It also suggests the creation of a compensation fund, potentially financed by designers and programmers, for cases where the owners of robots failed to take out insurance. Lastly, the resolution calls for the mandatory registration of all autonomous robots placed on the market to ensure traceability and transparency where these robots would cause damage.

Many European legal commentators are pondering over the necessity of new liability rules for robots. Indeed, according to some, the rules that already exist in the domestic laws of the Member States are sufficient to tackle the arrival of "intelligent and autonomous" robots. In direct response to the European Parliament's resolution, a statement was published by over 150 political leaders, AI/robotics researchers and industry leaders, physical and mental health specialists and law and ethics professionals to criticize the adopted approach. In their view, "creating a legal status of electronic 'person' would be ideological and nonsensical and non-pragmatic." If one analyzes the works of French legal commentators, a lot of them believe that the liability rules for damage caused by others (children or animals) could be sufficient and be applicable to autonomous robots.

* * *

As innovations in 3D printing, artificial intelligence, and IoT continue to develop, so will products liability law. Though the law lags, it is evolving. Developments should be closely monitored.

About the Authors

Stephen G.A. Myers *is a partner in the pharmaceutical and medical device practice group at Irwin Fritchie Urquhart & Moore, LLC.*

Sylvie Gallage-Alwis *is a partner and chairs the product liability practice at Signature Litigation in Paris.*

David L. Ferrera *is a partner and chairs the product liability litigation practice group at Nutter McClennen & Fish LLP.*

Richard J. Underwood *is a manager at Exponent Inc.*

Annie Huang *is an attorney in the intellectual property and technology litigation practice group at Robins Kaplan LLP.*

Rayna E. Kessler *is an attorney in the mass tort practice group at in Robins Kaplan LLP.*