Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 33 • NUMBER 7 • JULY-AUGUST 2021

Regulators Likely to Focus on Hybrid Transactions and IoT Devices

Stephen C. Piepgrass and Daniel Waltz

Consumers used more connected devices in 2020 than any year before it. As daily routines adjust, consumers spend more time at home, and as technology continues to evolve, consumers have quickly adopted smart devices to keep them connected to a wide variety of specialized services through the Internet of Things ("IoT"). One pre-pandemic study[1] predicted that more than 31 billion IoT devices would be in use at the end of 2020 (up from seven billion in 2018), and as many as 75 billion devices will be connected by the end of 2025. Industrywide, IoT devices manufacturers are operating in a new frontier – both industrially and legally.

The National Institute of Standards and Technology ("NIST") describes an IoT device[2] as one that involves "computation, sensing, communication, and actuation. . . . IoT involves the connection between humans, non-human physical objects, and cyber objects, enabling monitoring, automation, and decision making."

In other words, an IoT device has both physical and electronic components that exchange data over the internet to provide a service. By combining complex physical products with sophisticated services, manufacturers are revolutionizing how people interact with their environments and with one another. Well-known examples of IoT devices include everything from exercise bikes and treadmills, which allow the consumer to participate in online spin or running classes, to doorbells with integrated cameras that allow homeowners to view visitors at their doors – regardless of whether they are at home or on vacation.

When a consumer purchases an IoT device, they purchase the physical component because it facilitates useful services without which the device would not be as desirable. This transaction is sometimes called a "hybrid transaction" because it involves the sale and purchase of goods, software, and services in one bundle.[3]

But what happens when the device fails to perform as promised, causes harm, or the manufacturer ceases to support the product or goes out of business? The legal consequences are not uniform or well defined at present.

Stephen C. Piepgrass, a partner in the Richmond, Virginia, office of Troutman Pepper Hamilton Sanders LLP, represents clients interacting with and being investigated by state attorneys general and other enforcement bodies as well as clients involved with litigation, particularly in heavily regulated industries. **Daniel Waltz** is an associate in the firm's office in Chicago. The authors may be contacted at *stephen.piepgrass@troutman.com* and *daniel.waltz@troutman.com*, respectively.

IoT DEVICE LEGAL CHALLENGES ARE UNIQUE

Traditionally, sales of goods are governed by Article 2 of the Uniform Commercial Code ("UCC"), which standardizes commercial law to facilitate transactions across state lines. Unlike a transaction for the pure sale of "goods," transactions for the provision of services are not traditionally covered under UCC Article 2.

Instead, transactions for services are governed by a patchwork of common law precedent and inconsistent state laws and regulations. IoT devices, which involve the sale of a product and a service, make matters even more uncertain. Consumer transactions involving areas of legal uncertainty create an environment ripe for regulatory enforcement.

Many recent examples illustrate the potential legal and regulatory perils currently faced by manufacturers of IoT devices. Consumers willing to pay a premium for IoT devices are not happy when those devices fail to deliver the services they are designed to facilitate. Such consumer grievances frequently make their way into the press or to regulators paying attention to this space.

Several recent examples highlight potential areas of legal risk for manufactures as they engage in transactions for IoT devices in the United States.

IoT Devices That No Longer Perform

Unable to go to the gym throughout much of 2020, consumers have turned to internet-connected, at-home group exercise equipment. These exercise devices provide the hardware for a workout, while connecting users to a community of trainers and athletes who provide an enhanced at-home experience. It is the combination of physical goods and unique services that commands premium market prices for connected equipment.

Flywheel provides an example of an IoT device manufacturer that could no longer offer services with the smart products it manufactured.[4] Flywheel's exercise bike was essentially "bricked" as a result of an industry legal dispute, not a product defect or flaw. A Peloton competitor, Flywheel manufactured exercise bikes with an offering of online streaming training classes. After Peloton and Flywheel settled a patent dispute, Flywheel had to shut down its support for the at-home exercise bike product. Consumers who paid around $2,000 for the interactive exercise machine could no longer access the streaming classes and fitness support features, and thus were functionally left with a traditional stationary exercise bike.

The Flywheel experience is not unique. Mergers, acquisitions, and legal claims will continue to result in the "bricking" of IoT devices. And as early generations of IoT devices age, consumers will learn to cope with product failure due to planned or unplanned obsolescence as continued support for older generation products becomes economically unfeasible. Even when a manufacturer does not intentionally terminate services, built-in security features may cause IoT devices to cease functioning as cryptographic security certificates expire at a pre-determined date.

As consumers begin to recognize that IoT devices have a limited shelf-life, manufacturers need to think holistically about the product lifecycle at the point of product inception from a legal perspective. Manufacturers must be prepared to set consumer expectations and plan for various contingencies that result in product expiration – planned or unplanned.

Given the current unsettled legal environment involving transactions for IoT devices, manufacturers should be clear in their public-facing literature and contractual provisions. In the event of an investigation, regulators will focus on protecting consumers, taking into account the expectations established in the documentation provided by the manufacturer.

Devices That Can Be Modified Remotely by the Manufacturer

A manufacturer's ability to selectively turn on and off certain features of connected devices presents another area of unsettled legal risk for manufacturers. With increasing frequency, connected devices are manufactured with many features that the manufacturer activates only when a consumer pays for the specific services offered.

For example, BMW recently announced[5] a new subscription service that would allow consumers to decide whether to pay for features, such as heated seats and adaptive cruise control. The features are physically present in the vehicle at the time of manufacture, but only activated when the owner pays a subscription fee to BMW. However, the manufacturer's ability to activate and deactivate product features on command raises questions about whether

the transaction carries unintended or unpredictable legal risk.

The new subscription-for-feature model is inconsistent with traditional concepts of automobile ownership and the durability of features equipped on vehicles at the time of manufacture. Traditionally a vehicle sold with cruise control, for example, would continue to have the feature available to the vehicle owner regardless of how many times the vehicle is sold in the secondary market. Similarly, a vehicle with heated seats would presumably maintain the feature for the life of the vehicle. Not so in today's world of connected vehicles.

Not only does this trend raise questions about the marketplace (i.e., can a purchaser of a used car rely on the features originally listed on the window sticker?), but it also raises questions about the liability manufacturers might have when consumers allege harm as a result of this new subscription model.

For example, what would happen if a consumer wrongly believed the vehicle's adaptive cruise control feature was enabled and experienced an accident as a result?

What if a feature like traction control could have been deployed for a driver driving on slippery surfaces, but the driver had not paid for the subscription (or the manufacturer erred in failing to activate the feature)?

As the new model of connected automobiles (and other devices) is more widely adopted, manufacturers, sellers, and resellers will likely face increased regulatory scrutiny as a result.

Devices That Create Risk for the Consumer

Many IoT devices are susceptible to security risk. As an end-point device, IoT products are less secure than their computer counterparts from both a design and user standpoint. While a hacker cannot access your home computer directly, connected devices such as smart TVs, smart light bulbs, security cameras, and thermostats may provide a way for hackers to access a home network to backdoor a network security perimeter and access a connected computer. For several years, the Federal Bureau of Investigation has highlighted risks associated with smart devices to educate manufacturers regarding best practices, while encouraging consumers to exercise good judgment and be conscientious when using smart devices.

As medical device manufacturers adopt IoT technology to provide improved personalized services, it is apparent that even such devices are not immune from risk. For example, a pacemaker once used simply to maintain a regular heartbeat, can now use the IoT to track heart functions and improve the health care provider's ability to administer efficient and personalized treatment.

However, pacemakers suffer many of the same vulnerabilities as other IoT devices, including vulnerabilities associated with manipulation by malicious third-party actors. In 2017, the U.S. Food and Drug Administration announced a recall of nearly 500,000 pacemakers after it was discovered that a hacker could potentially gain remote access to the pacemaker.[6] Malicious activity could drain the battery quicker than expected or cause device failure with catastrophic consequences for the wearer.

One thing is clear in today's connected world: Devices connected to the internet are susceptible to increasingly creative threat actors. No system is perfect, and sophisticated threat actors can target even the most secure entities, including the U.S. government (as evidenced by the SolarWinds attack).

Manufacturers of connected devices must carefully plan for such eventualities and develop internet-connected devices in a legally defensible manner.

Additionally, manufacturers need to be careful in drafting their agreements to carefully define liability for security-related product failures. This can be difficult in a changing legal and regulatory landscape that has not caught up with technology.

REGULATORS WILL BE INSTRUMENTAL IN DEVELOPING THE LAW RELATED TO HYBRID TRANSACTIONS

As previewed above, UCC Article 2 governs transactions for the sale of goods and provides manufacturers of goods with predictability and uniformity across nearly all U.S. jurisdictions. Businesses can engage in cross-border transactions with the expectation that the terms of any agreement will be enforced uniformly regardless of jurisdiction. As a result, U.S. businesses can carefully structure their relationships, which allows them to anticipate their legal obligations and thrive despite the persistence

of legal risk. The UCC-offered uniformity also allows regulators to generally avoid interfering in well-structured commercial transactions.

Hybrid transactions, however, present novel legal challenges possibly not addressed by traditional UCC principles. The novel issues hinge on whether the sale of an IoT device constitutes a transaction for goods, governed by UCC Article 2, or a transaction for services not governed by UCC Article 2.

Courts have provided mixed guidance in this regard, adding further confusion to the legal landscape. Some courts have held that UCC Article 2 applies to sales transactions involving the sale of goods and non-good services bundled into a single transaction, while an equal number of courts have found that transactions that involve software constitute agreements for services not governed under the UCC.[7]

While the ideal solution (from a policymaking perspective) to the uncertainty surrounding hybrid transactions would be the adoption of a uniform legal system (e.g., modifications to the UCC, a separate uniform code, or federal regulations), that is not likely to occur in the foreseeable future.

In practice, the legal landscape will be developed as manufacturers of IoT devices encounter legal challenges and regulatory enforcement actions based upon developing interpretations of existing law by regulatory bodies, such as the Federal Trade Commission, Consumer Financial Protection Bureau, and state attorneys general. These enforcement actions will, in turn, lead to the development of new legal standards and an emerging regulatory landscape for the developing industry. While the path forward might be unclear at present, one thing is clear: The current landscape presents an irresistible target for regulators looking to define and shape an industry.

Regulators understand their role in shaping law and policy and will be interested in how best to address these novel legal issues in a way that allows future innovation and protects consumers.

Anticipating enforcement actions, IoT device manufacturers and marketers would do well to prepare by creating and implementing defensible industry standards.

Notes

1. *https://leftronic.com/internet-of-things-statistics/*.
2. *https://csrc.nist.gov/publications/detail/white-paper/2018/10/17/iot-trust-concerns/draft#:~:text=The%20Internet%20of%20Things%20(IoT,%2C%20automation%2C%20and%20decision%20making*.
3. Stacy-Ann Elvy, "Hybrid Transactions and the Internet of Things: Goods, Services, or Software?," 74 Wash. & Lee L. Rev. 77 (2017).
4. *See https://www.theverge.com/2020/2/20/21145349/flywheel-bike-shut-down-email-user-reactions-peloton-trade-in*.
5. *See https://www.businessinsider.com/bmw-subscription-model-for-features-2020-7*.
6. *See https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals*.
7. *Cf. Attachmate Corp. v. Health Net, Inc.*, No. C09-1161 MJP, 2010 WL 4365833, at *2 (W.D. Wash. Oct. 26, 2010) (finding that common law, not the UCC, governs transactions for software) and *Rottner v. AVG Technologies USA, Inc. et al.*, 943 F. Supp. 2d 222, 230 (D. Mass. 2013) (finding that the sale of software is akin to the sale of a good, and therefore, the UCC warranty provisions apply to the dispute).