Merton Howard and Shannon Nessier Hanson Bridgett LLP

FORECASTING LIABILITY WHILE CONNECTING TO THE INTERNET OF THINGS

For years, movies and television shows have depicted a future where every aspect of human life is sped up, controlled by the push of a button, and managed by speaking to a computer. We may not yet have instant transport tubes, but push the right button on your smart device, and your car schedules its own oil check, your door unlocks itself for an early-arriving guest, or your insulin pump notifies your doctor of your blood sugar level. And, every day, the Internet is a-buzz with the next time-saving, life-changing technology controlled by your voice or your phone.

The Internet of Things (IoT) refers to the ability of everyday objects to connect to the Internet and each other to send and receive data. IoT applications are rapidly being deployed in everything from consumer personal fitness products, to farming equipment, automobiles, toys, implanted medical devices, transportation logistics, smart cities, and security cameras. Companies participating in the race to connect should not overlook important legal challenges. Privacy and security issues are paramount, but there are other legal issues to consider, including regulatory compliance, insurance coverage, class actions, and product liability. The pioneering technology and vast collections of data present many exciting opportunities and conveniences. However, this connected web is fraught with vulnerabilities for product manufacturers, distributors, retailers, users, and insurers. Participants in this space must be mindful as they push forward with smarter technologies.

WHAT'S ALL THE FUSS?

The IoT is simply the term for the collection of Internet connected smart devices, which, through the use of embedded sensors, communicate specialized data to other technologies. The data is collected by devices, run through and often stored in the cloud, and used for analysis, feedback, and/or control of an object. Garbage cans send notifications when full; appliances call for maintenance; smoke alarms send a text when the alarm goes off; a beacon locates a stolen item; sensors on valves provide an alert when leaks are detected. When these devices are connected, each device, each transmission, and all the attendant data present possible exposure for the IoT industry.

There are four major areas experiencing increased legal involvement in the world of the IoT: regulatory compliance, product defect/malfunction suits, labeling/false advertising claims, and data breach/security.

Regulatory Oversight: While the federal government has been hesitant to issue IoT directed regulations, device and application creators have not gone unchecked. Many devices and their intended uses fall under general or industry specific regulations, while new guidelines have developed to fill gaps. For example, the Federal Trade Commission (FTC) issued a comprehensive IoT report, advising companies to build privacy and security into products/services at the outset, collect and keep only what is needed, provide clear and truthful notices and representations, and give consumers choices about data uses that are not obvious. The National Highway Traffic Safety Administration (NHTSA) modified its research organization to focus on vehicle electronics, including cybersecurity, and established a division to conduct research on the safety, security, and reliability of interconnected, electronic vehicle systems. And the Food and Drug Administration (FDA) has taken steps to strengthen the cybersecurity of medical devices, including the issuance of guidelines for Mobile Medical Applications.

As connected devices become the norm, we can expect increased regulatory action. Thus, before bringing these technologies to market, stakeholders must be educated about regulations, guidance, and trends.

Product Liability: Though pioneering, the IoT still involves the design and function of traditional, tangible products. To that end, many liability issues are not that different from those faced by traditional product industries. Whenever devices cause injury to person or property, traditional defect claims will commence. If a connected door lock fails, homeowners will seek property damages. When a connected CO2 monitor leads to respiratory issues, personal injury claims will follow. However, parties may be unsure about how blame will be allocated. Was it the hardware, a sensor, the phone application interface, the data transmission, or the user? Far more complicated than traditional manufacturer versus supplier disputes, these claims may drag all of the players into court, since they presumably have superior access to data (*i.e.*, knowledge). This will be especially true when dealing with industries holding highly protected proprietary information, to which no claimant would have pre-litigation access.

Labeling / False Advertising: The IoT has already seen actions aimed at marketing claims and warranties. High-profile wearable companies face claims that their fitness trackers do not provide the advertised level of diagnostics and feedback. Connected cars are targets even though no one has suffered bodily injury. For many false advertising and warranty claims, the nature of the damages suffered and the claims alleged make them vehicles for costly class actions. Though any one purchaser's damages may be worth pennies, the aggregation of pennies combined with attorneys' fees and penalties can cost a company millions, not to mention loss of good will and brand diminishment.

Data Security: The IoT works best when personalized data is leveraged for a custom user experience, but that requires companies to collect and store more and more data, exponentially increasing the already sizable task of managing and defending against data breaches. Whether data is stolen from the cloud, captured during transmission, or mined from a device, the increasing number of places the data is located will result in amplified vulnerabilities. Because the types of IoT devices continue to expand, reaching more intimately into people's homes and lives, and touching on more complex subjects like financial management, personalized healthcare, or municipal systems, the damages caused by breaches will dwarf those of recent years. It will not just be theft of a name or credit card number, but unauthorized control of an implanted medical device, access to water monitoring systems at a hydro-electric plant, or manipulation of vehicles in motion. As technology gets smarter, so too will those looking to abuse the data flowing through the connections.

SPECIAL CONSIDERATIONS

There is so much uncharted territory in IoT litigation that litigants, stakeholders, and even the Courts are left to make the best decisions they can on fairly novel issues. Without unified regulations or policies, this piecemeal approach will continue for the foreseeable future.

For example, litigants and courts must manage discovery of stored data on devices and in the cloud. While some data will likely be relevant and even essential to claims, the volume of data will be expansive, and the complication of mining it from what are likely several protected business and trade secret algorithms, hardware, and/or software locations makes the use of the data much more complicated than simply turning over a burned hair drier or blown tire.

Stakeholders also must consider whether they have adequate insurance coverage for their roles in the world of connected devices. Emerging companies are looking to avoid costly counseling on the front end, hoping to ask forgiveness after a product's success rather than permission in advance. In the insurance arena, this can be costly, even to the extent of risking the financial health of the entire company. In addition, while one party in the IoT chain may have the necessary coverage, it might partner with another company that does not. Likewise, a company's reaction to an issue, like a data breach, may itself cost them coverage. As the commercial players and insurance industry try to keep pace with developing technologies, both will get savvier about navigating coverage issues.

Finally, the number of stakeholders who might be involved in these claims could be fairly significant. Depending upon the nature of the malfunction or breach, litigants might seek damages from the manufacturer, seller, cloud storage provider, service providers, software licensors, device inventor, application creator, and untold others who played a role in bringing the IoT device to market. Managing these players and the issues specific to their industries and technologies will take lawyers well-versed in this field.

WHAT TO DO NOW?

Because of the sophisticated nature of the devices in the IoT, there is no single fix for the stakeholders seeking to protect themselves. But, there are a few strategic choices that will help minimize risk. First, do not overpromise in device and application marketing. Making accurate claims will be key to defending frivolous consumer suits. Second, stakeholders should consider insurance requirements and indemnity agreements with their stream of commerce collaborators. Given the number of parties involved, a clear assignment of liability will help manage exposure and simplify decisions during litigation. As with traditional product considerations, companies must label their products with any warnings or caveats, and follow regulatory guidance and rulings to assess appropriate standards of care. Disclaimers may not bar litigation, but they could help narrow the scope of available claims and damages. Finally, any party involved in data collection, storage, or transfer must have a data breach protocol ready to go. Planning for the worst and being prepared to respond in a way that shows the company in the best light will be key to restoring the company's good name, market presence, and profitability in the event of an IoT related incident.

Merton Howard chairs the Litigation practice at Hanson Bridgett LLP, a San Francisco-based firm. He represents businesses in commercial disputes, mass tort and product liability litigation, and claims involving California's Proposition 65, unfair competition, and premises liability. Additionally, he assists clients with regulatory compliance, product labeling, and crisis management.

Shannon Nessier is a litigation senior counsel at Hanson Bridgett in San Francisco. Her work concerns defense of product manufacturers and suppliers and premises owners in personal injury litigation. In addition, she provides advice and litigation defense on matters involving warning label claims, Organic labeling issues, and Proposition 65 claims.