



BEWARE OF THE IoT

BY PAUL BENT

Paul Bent is back with a history lesson on the “Internet of Things” as well as an update on protecting your firm from the liability of data collection, internet connectivity and potential threats to equipment assets in the ever-connected world of the internet.



PAUL BENT
Senior Managing Director,
Legal Services & Business
Quality Assessment
The Alta Group

The internet has come a long, long way from the vision of its founders. In 1969, when the first node of the ARPANET on the campus of UCLA delivered a one-word message, “login,” to a special purpose computer at Stanford University,¹ few would have predicted the internet of today. Originally intended as an experiment in packet switched communications and the then brand new TCP/IP switching protocol (funded by the U.S. Department of Defense), the internet, when it became fully operational in 1971, was essentially just a small scale government science project, providing file sharing and limited email among a handful of local networks with no civilian applications, no world

wide web, no graphics, no audio and no hint of what was to come.

Today, of course, about 5.25 billion people worldwide (more than 66% of the entire population of the Earth) have access to and use the internet frequently, and there are more than 157 million websites operating on the internet through the medium of the World Wide Web. Last year, more than 300 billion emails were sent throughout the world every day, and every minute, Americans generate 3.2 gigabytes of internet traffic.² And, in contrast to the first internet message, which could only be used by or be useful to two permanently installed multi-million dollar computer

systems, today, 54.4% of all worldwide traffic on the internet is conducted by mobile devices — 7.26 billion of them, or one for every one of about 91.5% of the world's population.

While this exponential growth in internet use continues apace, one particular segment of it is perhaps of even more importance to the equipment leasing and finance community — or at least it should be.

THE INTERNET OF THINGS

The notion of connecting sensors and intelligence from autonomous physical objects (as opposed to human-controlled computers) over the internet was first discussed back in the 1980s when a group of Carnegie Mellon graduate students set about to attach sensors to a Coca-Cola vending machine so they could remotely track its contents via the main computer of the university's computer science department and find out if there were any more drinks available. The rig was pretty primitive, but by 1999, a Proctor & Gamble computer scientist, then working at MIT, proposed attaching radio-frequency identification (RFID) chips to consumer products as a means of remotely tracking them via the internet throughout the company's supply chain. He coined the term "Internet of Things" (IoT), and a new buzzword — and the very beginning of yet another new revolution in technology — was born.³

What we now know as the IoT began its expansive growth in the early 2010s, when businesses started to see the potential for the IoT

“ We are all deep into the age of the internet, and the more we know about how it is expanding and becoming more pervasive through the IoT, the better we will be able to deal with whatever threats may come at us through cyberspace.”

to provide major improvements and financial benefits in their supply chains and inventory tracking. Then, as the internet itself expanded and became exponentially faster, additional manufacturers and service providers began to find more and more new uses for remotely connected devices, sensors, monitors and equipment.

Today, there are more than 10 billion devices actively connected to the IoT, and it is estimated this number will surpass 30 billion by the year 2030. Experts forecast that by 2025, we will see more than 152,000 IoT devices connecting to the internet every minute. They will collectively be generating more than 73 zettabytes of data⁴ and will have the potential to generate more than \$10 trillion in economic value. And many millions of these devices will be attached to or embedded in equipment finance or owned by leasing companies, gathering, storing, delivering and reporting trillions of bytes of someone else's data every minute of every day.

WHY ALL THIS MATTERS

As more and more items of personal property and equipment are festooned with IoT sensors and monitoring devices, they represent the potential for gathering, storing and reporting potentially huge volumes of data that will be collected, analyzed, utilized and stored by a wide variety of humans, including engineers, product developers, maintenance and repair personnel, software designers, safety and security officers and many more.

Of course, all this data may also be intercepted and exploited by hackers, thieves, con artists, saboteurs and other nefarious actors. Drawing from the history of other types of leased and financed assets, including transportation, automated manufacturing, high tech medical and other types of equipment that by their nature interact with people, it can be seen that the bad consequences of their negligent, harmful or improper use may fall in the laps of lessors and financing companies, and the parties who finance or

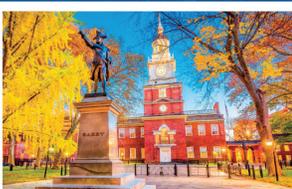
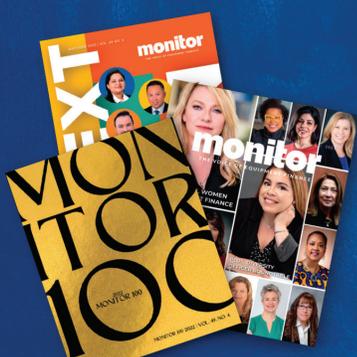


Save the Date

Next year will mark 50 years since the very first *Monitor* was published. Join us to celebrate *Monitor*, equipment finance, all of the extraordinary people who built our industry and those who are leading us into the future. Be sure to save the date!

June 15, 2023

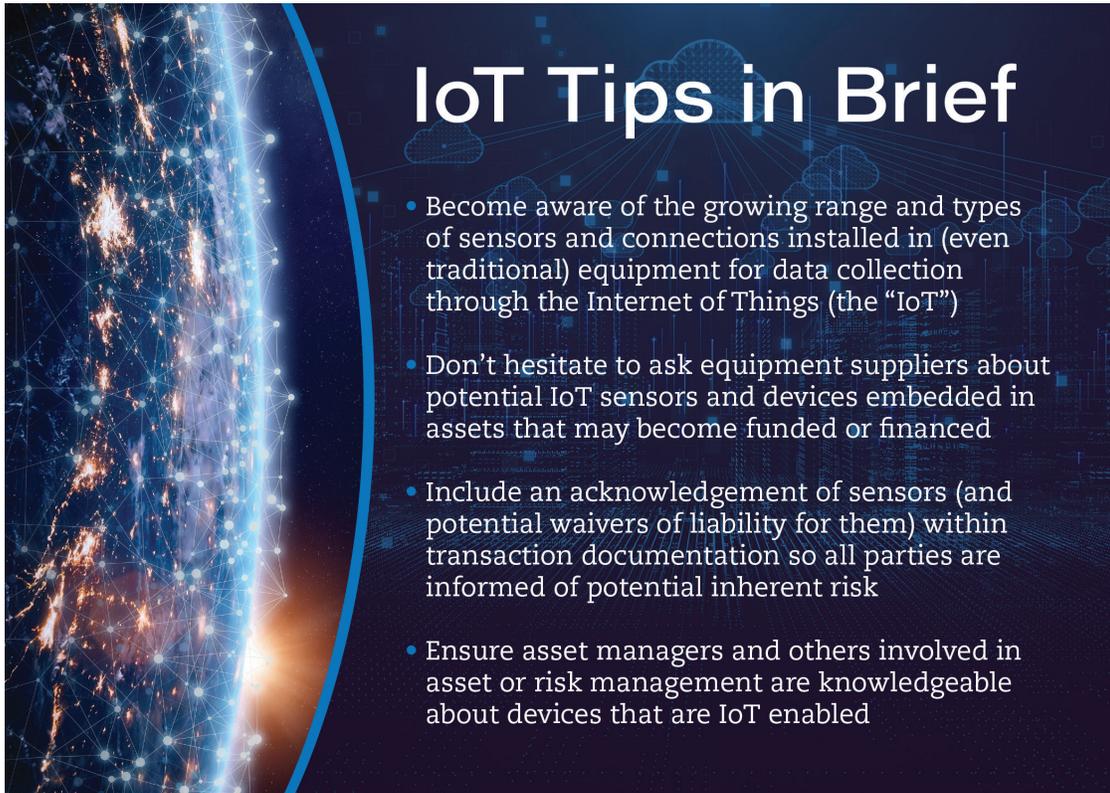
Monitor's 50th Anniversary Gala
National Constitution Center
Philadelphia | 6-10 p.m.



COCKTAIL RECEPTION | FULL COURSE DINNER | AWARDS CEREMONY |
EXHIBITS | INDUSTRY ROUNDTABLES | KEYNOTE SPEAKER | ENTERTAINMENT

For information regarding ticket sales, please visit
www.monitordaily.com/50th-anniversary-gala-2023

For sponsorship information, please contact Susie Angelucci at
susie.angelucci@monitordaily.com



IoT Tips in Brief

- Become aware of the growing range and types of sensors and connections installed in (even traditional) equipment for data collection through the Internet of Things (the “IoT”)
- Don’t hesitate to ask equipment suppliers about potential IoT sensors and devices embedded in assets that may become funded or financed
- Include an acknowledgement of sensors (and potential waivers of liability for them) within transaction documentation so all parties are informed of potential inherent risk
- Ensure asset managers and others involved in asset or risk management are knowledgeable about devices that are IoT enabled

own the equipment from which IoT data are gathered may be equally at risk in the event of any wrongful gathering, misuse or harmful use of these data, even if they have no knowledge of or participation in the actual use of the equipment, the IoT devices or the data.

Indeed, many legal claims have already been made against manufacturers and providers of wireless and remotely controlled devices for negligence in design and operation. As far back as 2015, class action lawsuits were filed against various auto manufacturers for selling vehicles whose onboard computer systems were “too easy to hack” and allegedly allowed third parties to control them remotely. Suits have been brought against hospitals and medical device providers for their alleged failure to protect implanted units such as pacemakers and heart re-synchronizers against hacking and outside interference. Home security system makers have been sued for designing and installing equipment that could allegedly be turned off or disabled by hackers using simple third-party software.

Many equipment lessors are familiar with the issue of “vicarious liability” in the context of being sued or named in legal actions concerning the wrongful or negligent operation of equipment they have leased to others (e.g., buses or vessels), even though the lessors were passive financing entities and had no

participation at all in the operation of these leased assets. Fortunately, the potential for very harmful penalties in this regard has been limited through corrective legislation, but such claims remain fertile ground for plaintiffs’ lawyers, and they will only expand as the opportunities for harm caused by misuse or negligent use of those zettabytes of data collected from leased equipment continue to explode and find their way into more and more areas of business.

Imagine, for example, the operation of a leased railroad locomotive is being monitored (and perhaps even controlled) remotely via IoT-enabled sensors in its powerplant, brakes, bearings or couplers — and the internet coverage fails, or the sensors are installed incorrectly, or the responsible computers are hacked over the internet. Being a potential third-party “deep pocket” in this scenario is very likely to put the lessor of the locomotive on the list of defendants if someone is harmed or if there is substantial property damage resulting from the failure or the hack.

Or, consider a leased high-tech medical device such as an MRI scanner that is gathering large volumes of personal data for a patient during a scan and transmitting them via IoT-enabled sensors to a remote location for storage and analysis — and a hacker

intercepts the data, whether for material gain or for nefarious purposes (and perhaps for hundreds or thousands of patients altogether), and wrongfully discloses them to other parties. Could the lessor of the scanner be held liable for the damages resulting from this behavior (or for penalties or sanctions under various statutes and regulations covering the wrongful disclosure of personally identifiable information)? It is certainly within the realm of possibility, and the risk of exposure to such liability is likely only to increase as the use and application of IoT-enabled devices grows exponentially.

These examples may seem like nothing new. Equipment lessors have faced similar claims for liability for many years and in many contexts, but concern about claims based on misuse or negligent use of IoT devices stems from both their ubiquity and their subtlety. As the speed, availability and connectivity of the internet continues to grow, and as manufacturers and operators seek to improve performance and uptime through “predictive maintenance,” they can be expected to install increasing numbers of IoT-enabled sensors in their products to monitor and report performance, operation, wear and many other KPIs that help predict failure well before it happens. At the same time, plaintiffs’ law firms are known to be adapting to the future of the IoT as well, using experts to probe and

attempt to hack networks to find weaknesses that may be exploited legally, and legislators and regulators continue to subject businesses (and their service providers, potentially including financing companies) to potential liability for breaches of privacy and misuse of personal information.

WHAT TO DO

Taken together, all the factors described here mean lessors must be vigilant in their knowledge, understanding and application of IoT devices and sensors installed in "traditional" equipment assets. The future will include a broad and rapidly growing range of asset classifications that will be peppered with IoT sensors and connections. At the very least, lessors should not be hesitant to ask about and should be aware of these features, since they may represent liability exposure for lessors if not used properly or if they are susceptible to hacking or other misuse, particularly in true leases, motor vehicle TRAC financings and other transactions in which the lessor is considered to be the owner of the equipment for all purposes.

Another suggestion is to include in transaction documentation an acknowledgement that the leased equipment includes sensor devices or other features that may connect with the internet or other facilities external to the leased or financed equipment itself (and are not within the control of the lessee) together with a written waiver or disclaimer of any liability arising from the use or connection of the device to the internet or any other facility or from the use or misuse of any data or information generated by the sensors. This will at least put the lessee or obligor on notice that the lessor is aware of the inherent risk in this regard and perhaps will encourage plaintiffs' lawyers to think twice before simply naming the lessor as a deep pocket defendant.

Most importantly, a lessor's asset management personnel or similar service providers should be alert to and knowledgeable about the IoT devices that are part of the leased equipment so they may assess the likelihood of failure or breach of these systems and the lessor and its advisors may evaluate the risk of exposure to all the parties that may arise from the wrongful or negligent use of the massive quantities of data presumably generated throughout the useful lives of the equipment.

We are all deep into the age of the internet, and the more we know about how it is expanding and becoming more pervasive through the IoT, the better we will be able to deal with whatever threats may come at us through cyberspace.

IoT TIPS IN BRIEF

- Become aware of the growing range and types of sensors and connections installed in traditional equipment for Internet of Things (IoT) data collection.

- Don't hesitate to ask equipment suppliers about potential IoT sensors and devices embedded in assets that may become funded or financed.

- Include an acknowledgement of sensors (and potential waivers of liability for them) within transaction documentation so all parties are informed of potential inherent risk.

- Ensure asset managers and others involved in asset or risk management are knowledgeable about devices that are IoT enabled.

¹More precisely, the first computer delivered only a partial word — a two-letter message ("lo") — before it crashed, thus establishing both the lore of the internet as beginning with the message "lo and behold" and the reality that computers can't help but crash at the most inopportune times.

²Just for emphasis, that is 3.2 billion bytes of data passing through the internet every single minute, just in the United States.

³The computer scientist, British technology pioneer Kevin Ashton, said when he presented his idea to P&G executives, he included the word "internet" mainly as an inducement for them to attend and fund his program, since the internet was at that time a newly emerging and exciting concept, and the name stuck.

⁴Zettabyte is the name for one sextillion bytes of data, or the equivalent of 1 billion terabytes, or (as a number) one followed by 21 zeros.

Paul Bent is a seasoned equipment leasing executive who currently serves as senior managing director of The Alta Group and manager of its legal services practice. With several decades of experience as an investment banker, equipment leasing CEO and transaction attorney, Bent has participated in all facets of leasing and corporate financing.

PORTFOLIO PROTECTION. PERFECTED.

We ensure you're covered, even when your customers don't.

You require customers to insure their leased or financed equipment and vehicles, but what if a policy expires or is cancelled? Stop worrying about loss exposure with a program from American Lease Insurance: it includes blanket contingent coverage on your entire portfolio that automatically takes effect when other coverage lapses.

Underwritten by A-rated insurance carriers, the ALI ProgramSM provides property and liability coverage through the entire term of each contract from inception. Meticulous tracking ensures each asset in your portfolio is adequately insured, and that your customers pay only for the coverage you require.

With the ALI Program, your customers benefit from a convenient, affordable insurance option with exceptional customer service, while you receive complete portfolio protection and additional fee income. Fully automated and integrated with all major lease accounting systems, the ALI Program relieves your team from obtaining insurance documentation to focus on closing deals.

We'll safeguard your assets and help you boost income and productivity. Find out how ALI can work for you: call 888-521-6568.



American Lease Insurance
654 Amherst Road
Sunderland, MA 01375
888-521-6568
www.aliac.net