Emerging Theories of Liability in the Internet of Things Era

Devin Bates
dbates@mwlaw.com
(501) 688.8864

03/25/2024

The Internet of Things ("IoT") has ushered in a new era of connectivity and convenience, but with it comes a host of legal issues and emerging theories of liability. As IoT devices become increasingly ubiquitous in our daily lives, from smart homes to industrial control systems, the potential for security breaches, privacy violations, and other risks has raised questions about who should be held accountable when things go wrong. In this blog post, we will highlight some of the emerging legal issues that seem poised to become increasingly significant in technology related litigation going forward.

1. Efficacy of Security Measures: One of the most pressing concerns surrounding IoT devices is their sometimes loose security measures. Some IoT devices lack robust security, encryption, and/or privacy controls, making them vulnerable to cyberattacks and unauthorized access to sensitive personal information. This could give rise to risk for consumers and businesses alike, as attackers may exploit vulnerabilities to hack a user or compromise sensitive data. New theories of liability will be tested around the theory that organizations have a duty to account for these risks, and take steps to mitigate them.

2. Disposable Hardware and Cyber Vulnerability Management of Devices: Another challenge in the world of IoT is the prevalence of inexpensive hardware that is often treated as disposable. Unlike traditional computing devices that receive regular software updates and security patches, many IoT devices are not designed to be updated or maintained over time. This lack of ongoing support leaves devices vulnerable to cyber vulnerabilities and makes it difficult for manufacturers to address security issues after the fact. To the extent that an organization's IT policies and procedures allow for individual employee use of personal hardware for organizational tasks, or to the extent that an organization purchases and assigns out various pieces of inexpensive hardware, some organizations will find it necessary to ensure that sensitive data generated by and stored on such disposable hardware is sufficiently safeguarded and scrubbed.

3. High Number of Potential Entry Points for Malicious Actors: IoT devices can serve as potential entry points for malicious actors into other computer networks and systems. Once inside a network, attackers may exploit IoT devices to launch further attacks or gain unauthorized access to sensitive data. This underscores the importance of securing IoT devices not only for their own sake but also to protect the broader ecosystem of connected devices and systems.

4. Increased Monitoring of Data and Privacy Risks: The widespread adoption of IoT devices also raises concerns about increased monitoring and surveillance of individuals' daily activities. From smart home devices that track our movements to wearable fitness trackers that monitor our health data, IoT devices have the potential to collect vast amounts of personal information without consumers' knowledge or consent. This raises privacy concerns for individuals, and to the extent that an organization is in possession of the data, it could also lead to issues if the organization accesses or relies on that data in

some decision making. Consider for example a device that collects location data and shares that data with a device under the management of an organization's IT department. In a FLSA case, location data could be used to show that someone was or was not working at certain times. In an injury case, location data could be used to show whether an employee was acting in the scope of their employment at the time of an event. In an employment discrimination case, the data could be used to show information was available to an employer, or to prove that it wasn't. And especially if an organization accesses such data, in any of these examples a litigant may attempt to argue that the employer knew or should have known something, or defensively used to show that an employer in fact did not know something. These are some illustrative examples, but they all underscore that data collection, management, and use is *THE* issue of the future in some areas.

5. Concerns about Public Safety: Perhaps the most alarming risk associated with IoT devices is the potential risks to public safety. Malfunctions or hacking incidents involving IoT devices could have devastating consequences, such as self-driving cars crashing due to hacker interference or attackers disrupting IoT networks used to operate critical infrastructure. These scenarios catch the attention of regulators, who call for robust security measures and regulatory oversight to ensure the safety and integrity of IoT systems.

6. Algorithmic Discrimination: Lastly, there is growing concern about the use of algorithms in IoT systems that may lead to discriminatory decisions. Even unknowingly, companies may deploy algorithms that a person later claims can lead to a biased outcome that perpetuates inequalities and injustices in society. This raises important questions about accountability and transparency in algorithmic decision-making and the potential legal implications for companies that deploy biased algorithms. For example, in the past month the State of Connecticut introduced a bill requiring developers of high-risk AI systems to "use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination." Additionally, the bill prohibits dissemination of certain synthetic images. Connecticut is one of the latest, but not the only, state to address alleged algorithmic discrimination with state law solutions.

In conclusion, the rise of IoT technology presents unprecedented opportunities for innovation and connectivity, but it also presents new risks and potential legal challenges that test a range of emerging theories of liability. As the IoT continues to evolve, new laws and regulations will emerge, and court cases will test the metes and bounds of liability in this new era.

This content was generated in part by, and prepared for publication with the assistance of, ChatGPT.