REPRINT

CD corporate disputes

INTERNET OF THINGS: EMERGING TECHNOLOGIES AND LIABILITIES

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
JUL-SEP 2020 ISSUE

www.corporatedisputesmagazine.com

Visit the website to request a free copy of the full e-magazine

SHOOK HARDY & BACON

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

www.corporatedisputesmagazine.com

ONE-ON-ONE INTERVIEW

INTERNET OF THINGS: EMERGING TECHNOLOGIES AND LIABILITIES

Russell Shankland
Partner
Shook, Hardy & Bacon
T: +1 (816) 559 2747
E: rshankland@shb.com

Russell Shankland has successfully litigated a robust range of complex commercial and tort claims in federal and state court. Beyond his courtroom experience, he brings valuable know-how related to e-discovery, records collection, review and production, and navigating discovery disputes. He has managed large review teams and oversees voluminous technology-aided reviews. Pro bono work also plays an important role in Mr Shankland's practice. He has represented adult defendants in federal and state criminal proceedings and children in juvenile proceedings, as well as working on civil rights claims.

CD: To what extent has the Internet of Things (IoT) pervaded our daily lives in recent years? How would you describe the evolution of this technology and the benefits it offers?

Shankland: The interconnectedness and interaction of devices promotes efficiency and precision and facilitates automation. That is true in industrial settings where the Internet of Things (IoT), alongside artificial intelligence and machine learning, are spurring a so-called fourth industrial revolution. It is also true for consumers. One in six Americans own a smart speaker. Upon waking, a person can make a simple command to the smart speaker and a customised series of events will commence. This may include cranking up the heat, playing the weather forecast, turning on the lights, starting the coffee maker and switching on the television, among other things. The smart home is about more than convenience, though. A person can be alerted of a smoke alarm, break-in or water leak from anywhere – or close the garage door or see and talk to whoever is at the front door. IoT devices remain in early stages, and it is hard to fathom the coming innovations that will surely touch on every aspect of daily life.

CD: How would you characterise the potential risks and concerns associated with the IoT? In the event of a connected device failing and causing harm, where might liability reside?

> **"As IoT reshapes the world, US jurisprudence stands underequipped to handle the challenges of evolving technology, balance inherent rights and resolve the unavoidable disputes."**
>
> *Russell Shankland, Shook, Hardy & Bacon*

Shankland: IoT devices are uniquely positioned to gather highly personal, intimate data about consumers, their habits, their relationships and their health. Cell phones alone track locations, store photos and video, monitor health data, connect to bank and credit accounts, transmit written communication, record voices and send all sorts of personal data to the cloud for storage. Smart speakers are always listening. Thermostats know when someone is home. Refrigerators monitor what people eat. Deadbolts can be unlocked from anywhere. What information devices collect

and transmit and what companies do with that information, including how they safeguard it and with whom they share it, is bound to lead to extensive litigation. This covers at least three areas. First, data security, such as data breaches. Second, data privacy, including sharing and use of data. Third, device security, where third parties gain unauthorised access to devices. It implicates potential liability for everyone throughout the supply chain, including manufacturers, vendors, cloud storage providers, data analysts, social media platforms and app developers.

CD: How can producers and designers best protect themselves from the liability risks associated with interconnected products?

Shankland: The first step is to design the device or platform to protect the security, confidentiality and integrity of personal information collected from or about consumers. This applies to engineering of hardware and software but also to implementation of policies and procedures for data security and privacy. The second step is to 'warn' customers. Customers should be informed how data will be used. But IoT devices are also like other products with associated risks. The maker of a device that tracks activity may warn that the device does not detect certain health conditions. The maker of a smart home device may warn that users need to implement internet security, like strong Wi-Fi passwords. The third step is to keep apprised of changing laws and legal trends, generally on data security and privacy and specifically regarding IoT devices. For example, Illinois passed a law in 2008 governing the collection of biometric information, but based on a recent decision finding, actual harm is not required, thus courts are experiencing a surge in litigation. In addition, a new California law went into effect that requires manufacturers of connected devices to equip devices with reasonable security features.

CD: Are existing product liability legal principles unfit to properly address interconnected products?

Shankland: As IoT reshapes the world, US jurisprudence stands underequipped to handle the challenges of evolving technology, balance inherent rights and resolve the unavoidable disputes. The law on data security is more advanced, while the law on data privacy is incipient. Common law theories based in privacy torts or contract law, though being tested, are not well-suited to address use of electronic consumer data. California became the first state to adopt a comprehensive consumer data privacy law. It grants individuals certain rights: to know what personal information is being collected, used, shared or sold, to have their personal information deleted, and to opt-out

of their personal information being sold. For data breaches, it provides a private cause of action, but for data privacy violations, the attorney general must bring an administrative enforcement action. Federal statutes impose piecemeal data protection obligations on particular institutions and industries. Absent comprehensive federal law, the Federal Trade Commission (FTC) is using its broad, but debatable, authority to bring administrative and judicial actions against companies for handling of consumer data, relating to data security and data privacy.

CD: What data privacy issues does the IoT engender? Given the very real threat of hacking and security lapses, what steps do companies need to take to limit potential damage and associated liability?

Shankland: Data breaches, identity theft, facial recognition, deep fakes, cyber security and data misuse make headlines. But legal questions like whether people own their data or can control what data is collected remain unanswered. The Supreme Court has not recognised an individual right to data privacy. Only recently has such a right come to the forefront of the legal landscape. Interestingly enough, the privacy rights being recognised are not rooted in the Constitution. In the US, they are being enacted by state legislatures or enforced by regulatory bodies. Companies working in the IoT space, especially those dealing with consumer data, should consider developing a formal information security and privacy programme. Such a programme may include implementation of policies and procedures to protect data and routine auditing and reporting to ensure conformity. Companies may want to conduct data security and privacy reviews before new products or services are introduced. They may even designate compliance officers for the programme.

CD: From a product liability point of view, what should companies consider including in their written contracts? What information should be provided to end users and other related parties?

Shankland: Companies should inform customers of how data will be used and get the consent of those customers. In the digital world, consent often takes the form of privacy policies, terms of service or user agreements. Effective consent will likely negate contract and tort claims based on data privacy, but the form and scope of the consent matter. That is, the customer needs to have consented to substantially the same conduct. Some privacy policies, terms of service and user agreements for IoT devices are elusive, vague, unclear, lengthy or missing critical information. And those contractual documents change frequently. Just because a consumer has consented to one version does not mean that the consumer consents to later versions.

When companies share data with third parties, they should delineate what the receiving entity may do with the data and, where appropriate, impose reasonable protections preventing the receiving entity from misusing the data.

CD: How do you envisage liability issues associated with IoT unfolding in the years ahead? What legal and regulatory developments do you expect to see – and how should companies prepare to respond?

Shankland: For consumer data collected using IoT devices, a patchwork of incongruent state statutes benefits no one and creates compliance nightmares. Companies will grow weary crafting distinct practices and procedures that apply only to one state. Similarly unsatisfactory is the Food and Drug Administration (FDA) employing a questionable mandate and imposing vague, long-lasting obligations. The FTC can only bring actions based on violations of preexisting law or a company's own policies. Most companies settle, and the resulting consent decrees often cover a period of 20 years into the future and allow the FTC to conduct continuing supervision. Common law theories have only circumstantial application. A comprehensive approach on the federal level provides the most promise. Measures have been proposed in Congress; none have gained momentum. Eventually, proliferation of IoT devices, and ensuing disputes about data security and privacy, will force action. When that happens, it will be important to apply lessons learned from the California Consumer Privacy Act (CCPA) and the EU's General Data Protection Regulation (GDPR) and to carefully balance the individual right to data privacy with the substantial burdens placed on those obligated to comply. CD