Cyber Security Meets Product Liability

Melody McAnally
Memphis, TN

More and more products are becoming part of the "Internet of Things" ("IoT") – products that connect, store or transmit information via the Internet. Experts estimate that by 2020 there will be 50 billion IoT devices. Cars. TVs. Cameras. Home alarms. Baby monitors. Medical devices. Like all technologies, there are benefits and risks. It has become more and more apparent that all IoT products can suffer a cyber-attack. Remember that hackers have a variety of motives. Damage to reputation. Competitive advantage, particularly with nation states. Embezzlement. Theft of trade secrets and IP.

But does poor cyber security mean product liability? If so, how should IoT manufacturers prepare to defend a product liability lawsuit?

IS THERE A PRODUCT DEFECT? Is an IoT product defective because it is hacked? This will certainly become a battle of the experts. For courts applying a risk-utility test, how will the courts measure a high cost of securing an IoT product from a cyber-attack? Does the state of the art require every IoT product to use the same security measures as, say, our power grid or military defense systems? Technology changes so quickly that an IoT product may be reasonably secure at the time of manufacture, but not at the time a consumer is using the product. For courts applying a reasonable alternative design theory, can a plaintiff show a reasonable alternative design that could have reduced or avoided a cyber-attack?

IS THERE AN INJURY? Is a cyber-attack itself an injury (assuming there is no personal injury)? If so, does the economic loss rule preclude liability?

IS THERE INSURANCE COVERAGE? If a manufacturer does not have a cyber policy, this seems more and more unlikely given the courts' current view of CGL insurance coverage in traditional data breach litigation. Especially if the product is used as a component in a larger product and the larger product is hacked. In 2014, the Insurance Services Office introduced a new set of exclusions that excluded coverage for cyber-attack related liabilities in traditional CGL policies.

There is also the risk of spoliation claims.

Product manufacturers should not wait for the courts to answer these questions. As the Federal Trade Commission ("FTC") recommends with all IoT devices, manufacturers should build reasonable security into IoT products at the outset, rather than as an afterthought in the design process. What constitutes reasonable security, of course, is an ever changing standard and varies depending on the sensitivity of data collected. While many future security needs cannot be predicted with certainty, here are some of the best practices suggested by the FTC.

1. **Start with a security risk assessment.** Identify the threats and vulnerabilities. Hire someone outside of your company to perform this assessment. As the saying goes, your internal IT employees "don't know what they don't know." Get a fresh set of eyes.

2. Minimize the data you collect and store. If your company does not need to store data for business purposes, don't! The more data you store, the larger target you are to hackers..

3. Test your security before launching products.

4. Monitor your products throughout the life cycle, update software, and patch known vulnerabilities if feasible.