How many THINGS do you have on the INTERNET OF THINGS? And more importantly, are your THINGS safe from cyber-attack?

Client Advisories

11.12.2018

Merriam Webster defines the Internet of Things ("IoT") this way: "the networking capability that allows information to be sent to and received from objects and devices (such as fixtures and kitchen appliances) using the Internet." While refrigerators and porch lights are easy to see as "things" that might be connected up to the Internet and thereby controlled at a distance, the IoT is much more than a way for turning off the air conditioning when one has already left town for vacation. Currently it is estimated that approximately ten billion devices are connected up to the IoT and that that number will triple in about three years.

While consumer devices are most commonly associated with the IoT, technological advances are rapidly bringing industrial systems and medical care facilities into the IoT, and therefore into the glaring spotlight of the possibility of cyber-attack, just as the effect that that glare has had on the banking and retail sectors of the economy. So as remote diagnosis of heart attack is becoming reality, for example, all of the problems associated with cybersecurity attacks must be addressed by a whole new range of potential victims.

As a result, in 2015 the Federal Trade Commission ("FTC") published a report that called on IoT companies to ensure that data collection, storage, and processing of customer data must be safe from cyber-attack.

While the FTC has yet to issue regulations in this area, the Information Technology Laboratory ("ITL") at the National Institute of Standards and Technology ("NIST"), an agency of the United States Department of Commerce, has published a draft report entitled "Considerations for Managing Internet of Things (IoT) Cybersecurity Risks and Privacy Risks." In the abstract of the draft, the ITL states: "Many organizations are not necessarily aware of the large number of IoT devices they are already using and how IoT devices may effect cybersecurity and privacy risks differently than conventional information technology (IT) devices do. The purpose of this publication is to help federal agencies and other organizations better understand and manage the cybersecurity and privacy risks associated with their IoT devices throughout their lifecycles."

Suffice to say, the draft is a treasure trove of information, even before being finalized, for any organization, corporation, or group that relies on devices that might not so obviously be "things" in the IoT, especially to understand and mitigate the risks inherent in three areas: (i) protecting device security; (ii) protecting data security: and (iii) protecting the privacy of individuals. The report is accessible at this link.

Archer's Data Privacy and Cybersecurity Group attorneys can help you navigate that report, as well as with your overall cybersecurity and privacy concerns, both from a preventive viewpoint and from the perspective of fixing things after the fact. If you have any questions, please contact Archer's Privacy and Cybersecurity Group members Gregory J. Winsky at 856-616-2610 or gwinsky@archerlaw.com or Robert T. Egan at 856-354-3079 or regan@archerlaw.com

Attachments