CARLTON FIELDS

NIST IoT Framework Raises Interesting Cybersecurity and Data Privacy Challenges

December 23, 2015

The National Institute of Standards and Technology (NIST) released the draft Framework for Cyber-Physical Systems, which is intended to provide an outline for the development and maintenance of secure, interoperable Internet of things (IoT) devices, also referred to as "CPS" devices. The Framework is designed to provide a common foundation for IoT applications across multiple industries, such as manufacturing, transportation, energy, and health care. Today's IoT continues to grow, and now includes devices such as smart cars, residential HVAC systems, and wearable devices. The comprehensive Framework addresses a variety of challenges, some of which may forecast potential legal concerns for IoT stakeholders. The Framework addresses the cybersecurity and privacy challenges that are inherent in all interconnected, data-driven systems. Because IoT devices connect cyberspace with the physical world, the Framework recognizes that "the mechanisms used to address IT challenges may not be viable in the world of CPS." The Framework further notes that the IoT presents significant privacy challenges. NIST's insights are telling of the coming legal and regulatory challenges that IoT companies may face. **Because of the way IoT devices allow individuals to interact with the physical world, a "privacy violation can be quite different from that of an information privacy violation," such as a data breach.** Companies that are trailblazing a path through this budding industry need to be cognizant of laws and regulations that affect physical—rather than purely digital—privacy concerns. In addition to new physical privacy concerns, IoT companies face increased exposure from typical cybersecurity risks. IoT data is "often collected for the sake of the management of the system, not for any userdriven purpose." Designers must consider what gains may be had in collecting and maintaining certain data versus the risks and compliance costs associated with that data collection. Companies pioneering IoT development should be mindful of all privacy and cybersecurity risks associated with the interconnection of cyberspace and the physical world. As the industry develops, companies will need to employ cutting-edge legal and compliance strategies to go along with their cutting-edge CPS products.

Related Practices

Cybersecurity and Privacy
Intellectual Property
Technology

Related Industries

Technology