LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
THURSDAY, FEBRUARY 14, 2019

PERSPECTIVE

Connected buildings, connected things and security considerations

By Scott M. Wornow

Is your "smart building" connected? Is your high-tech office, residential building or entertainment facility, with embedded sensors, wireless networks, remote monitoring devices and internet-capable security cameras, now just another "thing" connected to the global "Internet of Things"? Does embedding internet-connected devices within a building infrastructure impose enhanced "cybersecurity" requirements on developers, owners, architects, contractors or other building stakeholders? Do any of those stakeholders have affirmative obligations to mitigate the potential for breaches, hacks or misuse of embedded devices? While, perhaps, an odd question, the "connectedness" of buildings, cars and other "objects" requires renewed consideration of security protocols and practices in light of evolving laws, changing commercial expectations and the potential implications for ubiquitous connected "things."

California recently passed the first state law imposing security requirements on "connected devices." The law, effective Jan. 1, 2020 (to be codified at Title 1.81.26 of Part 4 of Division 3 of the California Civil Code), requires manufacturers of internet-connected devices (with exceptions for federally regulated and health care-related devices) to equip them with "reasonable security features." While ostensibly applying mainly to "off-the-shelf" wireless devices, like security cameras, thermostats and similar products with which consumers are fairly familiar, the definition of "connected devices" goes beyond the plain English. Under the new statute, "connected devices" also include any "other physical object" that is "capable of connecting to the Internet, directly or indirectly," and that is assigned an IP address or Bluetooth address. What might that broader definition capture, with nearly every physical object today embedded with wirelessly enabled electronics that permit the exchange of data through the internet? Refrigerators, toasters, coffee makers, smoke detectors, vacuum cleaners, door locks, electricity meters, and, indeed, even formerly "static" buildings, cars and trains all come today with an embedded capability that enables them to interact with the internet. And, of course, the ability to connect with the internet offers hackers the opportunity to enter those objects, to control those objects, to lock-down those objects, to extract data from those objects and to move from connected object to connected object within a network. In April 2016, internet users in Europe and North America experienced that susceptibility when a distributed denial of service attack against Domain Name System provider Dyn, Inc., which manages web addresses and routes internet traffic, resulted in several hours of extensive network outages. The malware responsible for that attack infected the Dyn network, and overwhelmed its servers, by taking control of nearly 150,000 connected devices, including wireless security cameras, lightbulbs and baby monitors. Experts suggested that the attack had been initiated by a lone disgruntled gamer upset with the Sony PlayStation game network.

If a building, entertainment facility or sports arena is wirelessly enabled with embedded sensors, cameras and other internetcapable objects that are designed with input from a developer or construction firm, and built to owner specifications, might that developer, owner or construction firm qualify as the 'manufacturer' of a physical object — the building, the arena, a room, a space, an office — that exchanges data with the internet?

The international research and advisory firm Gartner, Inc. estimates that by 2020, there will be 25 billion or more connected devices. PricewaterhouseCoopers estimates that nearly $6 trillion will have been spent by businesses and consumers between 2014 and 2020 on hardware, software and connectivity solutions for the Internet of Things. IDC Corporation predicts that the Internet of Things marketplace — software, services, hardware and connectivity — will reach $1.7 trillion in 2021. By all measures, the number and types of connected devices will increase exponentially and proliferate even faster. The cost of electronics components will continue rapidly to decline and components will continue to get smaller. Wireless speeds and network coverage will continue to improve, with next generation "5G" wireless networks nearly ready for commercial deployment. The collection, transmittal, storage and analysis of terabytes and terabytes of data through internet-enabled objects will continue to accelerate. The new California law, whether, intentionally or otherwise, demands that a broader cross section of stakeholders assume responsibility for, or, at least, consider the implications of lax, or non-existent, security within connected devices and objects.

Who qualifies as a "manufacturer" of an internet-connected object under the new statute? It seems rather uncontroversial to suggest that a "car" is today a connected device and that the automobile manufacturer has likely assumed a responsibility, legal and otherwise, for the design, manufacture and security of its wirelessly enabled, and potentially "hackable," transportation platform (that responsibility to the public stands independent of possible reimbursement claims the car manufacturer may have through customary third party indemnification arrangements with specific component manufacturers). Does a building owner, developer, architect or construction firm face similar questions regarding a networked facility that it has helped to create?

The statute applies to the "manufacturers" of "connected devices" and "connected objects" that are sold or offered for sale in California. If a building, entertainment facility or sports arena is wirelessly enabled with embedded sensors, cameras and other internet-capable objects that are designed with input from a developer or construction firm, and built to owner specifications, might that developer, owner or construction firm qualify as the "manufacturer" of a physical object — the building, the arena, a room, a space, an office — that exchanges data with the internet?

Connected physical objects are required to have "reasonable security features" that are "appropriate to the nature and function of the device," appropriate to the "information" that the device may collect and transmit, and designed to protect the device from "unauthorized access." "Appropriateness," as a legal standard, should be expected to evolve and should remain a constant source of inquiry. Beyond an overarching set of security principles, the statute provides that preprogrammed passwords unique to a device or features that require a user to create a new means of authentication before the device is first accessed will constitute "reasonable security features." But even if preprogrammed passwords or other authentication measures are implemented, the "appropriateness" of those measures to the nature and function of a particular device or object will remain subject to further consideration.

The California statute does not create a private right of action. It limits enforcement to the "Attorney General, a city attorney, a county counsel, or a district attorney." But while enforcement may initially be restricted, the effects of the statute, especially as the first of its kind in the nation, will no doubt be broad and the bar it establishes for security practices involving connected "things" will no doubt rise. If it seems a stretch to cast a building developer, owner or construction firm the "manufacturer" of a "connected object," the underlying legislative intent is clear — turning an intentional or unintentional "blind eye" toward cybersecurity protections for connected objects is unacceptable. Expectations have evolved; standards and practices will need to catch up.

The California statute, directly and indirectly, demands that anyone placing a connected object in the market for use by consumers or businesses undertake a critical security assessment of that "thing." With a statutory security framework for connected devices taking hold in 2020, and a heightened societal awareness occurring in parallel, is it, or will it become, "negligent" to design or install an embedded sensor network without appropriate security features? Are there, or will there arise, express or implied warranties regarding the security of embedded devices and sensors or wireless networks within newly constructed facilities? How far and wide among the engineering and construction stakeholders associated with a new building or facility will those warranties and obligations extend? Do legacy construction and design contracts effectively address responsibility for connected security? Will questions of device security eventually inform issues of occupant safety and habitability when, for example, sensitive network data or personally identifiable information is stolen, when internet-ready cameras are turned by hackers into voyeuristic tools, when ambient sensors are used to disrupt building cooling and heating systems or when medical refrigerators are remotely disconnected causing essential medicines to spoil? Did the builder, owner, construction manager, facilities operator or other vendors properly consider appropriate security features to incorporate into their connected object during the design or "build" stage? Whether the new California statute is applicable on its face or not, and whether it affords a private claim or not, the statute, if nothing else, requires anyone creating or developing an internet-connected platform, or making available a connected object, to consider and think proactively about the features and measures necessary to ensure appropriate security for the platform and objects they intend to interact with the Internet of Things.

Scott M. Wornow *is the former chief legal officer for several publicly traded technology companies and currently special counsel at Coblentz Patch Duffy & Bass LLP.*


WORNOW