July 21, 2014

Contact:
Timothy J. Toohey
Partner
213.417.5324
ttoohey@mpplaw.com

Privacy and Security Issues for Design Professionals in the Interconnected Building Environment

Ubiquitous connectivity, omnipresent tracking and monitoring, and the increased interconnectivity of systems mark the world we live in. As increasing numbers of non-traditional devices are connected to one another and to the Internet, paradigms for privacy and security are shifting, as are the expectations of the users of an interconnected environment. We are no longer in the Internet of ten years' ago – the Internet of computers and servers. We are now well into the "Internet of Things" era, where non-traditional devices, including mobile phones, wearable technology, and control systems for industry, transportation and the power grid are connected through and to the Internet. CISCO estimates that there are 10-15 billion connected devices on the planet today with more "things" than computers connected to the Internet. By 2015, it estimates that there will be 25 billion connected devices and, by 2024, 50 billion.

The types of connected "things" or devices vary considerably, but are all made possible by inexpensive RFID tags, chips and sensors, as well as connectivity and cheap storage of data. CISCO, which is understandably bullish about the phenomenon, describes the future as the "Internet of Everything" made up of the "networked connection of people, process, data and things."

Although the general public may be familiar with devices such as the Fitbit health monitor, Google Glass, or Nest "smart" thermostats, the Internet of Things also has implications for design professionals. The built environment increasingly is an interconnected or "smart" one employing sensors and interconnected devices and systems to achieve efficiencies. "Smart" buildings have rapidly increased in number because of the need for energy conservation and other environmental factors. Building control systems, which are at the heart of smart buildings, no longer rely on proprietary software and hardware, but on non-proprietary software connected through network technology with an Internet interface. Examples of such

technology include systems for managing energy consumption that sense building occupancy, wireless lighting control mechanisms, and systems for the reduction of lighting and energy loads. Other building systems, including fire-life-safety and security system, also increasingly have Internet interfaces.

With rapid advances in mobile phone sensors, the building control and other systems of the future may be triggered by individuals' mobile phones. An article in one technology publication notes that "the sensor-packed smartphone of the future [will be] part of a larger network of devices, whether it's the thermostat at home or the Wi-Fi enabled lamppost out on the street, each with their own integrated miniature monitoring components." Although mobile phones may be used as sensors in the home, they could just as easily be employed in other contexts, including office buildings and hotels, to detect building occupancy and control systems.

Advances in sensors and the increased interconnectivity of devices will likely produce considerable benefits, including energy efficiency and ease of control and use. As envisioned by Ericsson's "Social Web of Things," we will live in a world where our networked "smart" appliances interact not only with us, but with each other, to predict and react to our behavior. Although some find this inspiring, others find it reminiscent of the out-of-control computer Hal in *2001: A Space Odyssey*.

Although it is unclear whether the future of interconnected things will be a utopia or a dystopia (or both), there is no doubt that greater interconnectivity of devices is creating increased vulnerability from the point of view of both privacy and security. As a leading security organization has succinctly stated, "more connected devices means more entry points for potential hackers." When systems are integrated through the Internet, as opposed to being isolated from one another, sensitive and proprietary information may be exposed to unwanted eyes.

To choose an example familiar to design professionals, building management systems with IP address are increasingly accessed through the Internet. Although such access may make it easier for building occupants to request off-hours air conditioning, the exposure of these systems to the Internet makes them vulnerable to attack by unauthorized individuals. When a system is hacked, the hackers may not only gain control of proprietary or personal information, but be able to control the system remotely or

gain access to other aspects of a network. Such attacks may not only produce non-tangible results, such as loss of proprietary data, but, even more significantly, affect the security of the building and its inhabitants. Although there have not been many reports of such attacks, researchers were able to hack the building control system at Google's Australia offices in 2013 and to demonstrate the vulnerability of the system to Google. In this context it is also important to remember that in the well-publicized data security breach of Target, hackers gained access to Target's point-of-purchase payment system through an HVAC contractor with access to some part of Target's computer system. Other systems, such as security systems, are subject to the same types of vulnerability.

Individual devices are also subject to attack. As reported by security reporter Brian Krebs on February 18, 2014, the Belkin WeMo family of home automation devices gave "malicious hackers the ability to remotely control the devices over the Internet, perform malicious firmware updates, and access an internal home network." In a case which drew the attention of the Federal Trade Commission, TRENDnet, which sells home video and surveillance cameras, came under fire because its cameras had faulty software that allowed online viewing or listening by anyone with the camera's IP address. After a hacker exploited this flaw to post live feeds from 700 cameras online, the FTC brought an enforcement action against TRENDnet. Under its settlement with the FTC, TrendNet was prohibited from misrepresenting the security of the cameras or the privacy of information collected by its products, was required to establish a comprehensive information security program, had to notify customers about security risks, and was required to conduct biannual third-party assessments of security for the next 20 years.

Given the risks to security and privacy posed by interconnected devices and systems, it is important for design professionals to consider the security and privacy implications of interconnected building systems from the outset of the design process. One approach to the evolving privacy and design issues associated with interconnected systems is for professionals to adopt the privacy and security "by design" principles that have gained currency in other fields. The principles, which were developed by Ann Cavoukian, the former Information & Privacy Commissioner of Ontario, Canada, call for enterprises and individuals to: (1) be proactive, not reactive; (2) make privacy the "default" setting; (3) embed privacy into design and architecture of systems and business practices; (4) avoid false dichotomies (such as "privacy vs. security"); (5) embody end-to-end security before information is collected and extend it through the life

cycle of data; (6) keep privacy and security practices visible and transparent; and (7) respect user privacy by keeping practices "user-centric."

Although these principles are not applicable to all aspects of the work of design professionals, the ethos that they embody should and can be a focus of design practice. In designing and constructing smart buildings and the interconnected systems that are integral part of such buildings, design professionals should consider privacy and security implications of the design from the outset—not as an afterthought. Concern for privacy and security in the design profession not only serves the interests of clients, but also those who use, access, and are affected by buildings and building systems. Privacy and security "by design" is also a sensible risk management strategy. With increasing attention paid to privacy and security in an interconnected world, design professionals not only have a responsibility to respect those values, but would be well advised not to attract scrutiny from the government and clients if they do not live up to those obligations.

About the Author

Tim Toohey is partner with Morris Polich & Purdy LLP in Los Angeles and is the head of the firm's Cyber, Privacy and Data Security team. He is a US and EU Certified Information Privacy Professional (CIPP/US and CIPP/EU). Tim is the author of *Understanding Privacy and Data Protection: What You Need to Know* published in 2014 by Thomson Reuters/Aspatore. He is also the editor of the website www.privacydatasecurity.com.