October 24, 2018

LAW BUSINESS TECHNOLOGY
BUSINESS TECHNOLOGY LAW
TECHNOLOGY LAW BUSINESS
THE RECORDER
daily at www.therecorder.com
An ALM Publication

'Smart Cities' Raise Novel Issues and Novel Risks

By: Mark Raffman

The advent of "smart cities"—made possible by the burgeoning "Internet of Things" (IoT)—presents revolutionary opportunities for municipal planners and developers, and the private business enterprises partnering with them. Along with those opportunities, however, come new types of risks that should be taken into account by governments, businesses and affected interest groups.

By one estimate, the market value of investments in IoT tools and platforms to modernize cities around the world will exceed $2 trillion by 2025. See James Bourne, "Smart cities market value to hit $2 trillion by 2025, says Frost & Sullivan," IoT news, (April 4, 2018)). Connected devices can improve traffic control by easing traffic flow through traffic signal controls and providing access to "smart parking." Utilities can take advantage of remote sensors to measure and direct power flow and water usage, and can use motion sensors to provide "smart lighting." Connected devices are available to signal when industrial and institutional waste receptacles are full and in need of collection, reducing waste management costs. Sensors in public works such as bridges can be used to detect stress issues, seismic activity and other public safety parameters. See Michael Miller, "The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities are Changing the World" 265-79 (2015). Not only can connected devices be used to improve public utilities and public works, but the measurements they provide can in turn be used to guide decisions about development and investment. See Steve Olenski, "The Dos and Don'ts of Building a Smart City," Forbes, (Oct. 26, 2017). The result is better and more efficient management of traffic, public spaces, and public utilities, and more responsive policing and emergency services.

But there are challenges as well. The development of smart cities by their nature will involve new modes of interaction between private enterprise and public entities. As IoT devices become ubiquitous in public spaces, the stakes are raised for issues of privacy and security, particularly given the "political" dimension of much of the data that such devices generate. And the intersection of software with the physical world raises the specter that software glitches or hacking could result not just in devices that don't work the way they should, but that cause serious property damage or injury to life and limb.

Ownership and use of data generated by smart city technology will be a hot-button issue as public/private partnerships generate more and more data. Cities have data about all kinds of subjects, including income, crime, traffic, fires and emergencies, land use, parking citations, waste removal and so on. When government entities rely on private actors to generate or collect data in the context of a smart city, questions about ownership and use of such data become acute. Needless to say, the

(Photo: Courtesy photo)

Mark Raffman, Goodwin partner

data generated by a smart-city network can provide valuable insights into population patterns, consumer behavior, demand for services and other parameters that could easily be monetized—or misused. That such data are generated by or through a public entity sharpens the issues that surround data use and ownership, particularly in cases where there is a possibility that individualized data may be used for surveillance rather than serving individuals' needs. See Liesbet van Zoonen, "Privacy concerns in smart cities," 33 Government Information Quarterly 472-80 (July 2016)). Evolving technology—such as cameras embedded in light bulbs mounted on street lights—render the issue more than hypothetical. Stakeholders include the government entity, the private actors participating in shaping the IoT network and

gathering the data, the individual citizens whose behavior generates the data, and intermediary citizens' organizations such as condo associations or homeowners' groups.

As one example, consider a dispute that erupted when the city of Toronto partnered with a Google entity called "Sidewalk Labs" to create a 12-acre high-end waterside development (Quayside) as a prelude to developing a much larger 800-acre tract (Port Lands). The aim is to build an "advanced microgrid" to power electric cars, design "mixed-use" spaces to reduce housing costs, and employ "sensor-enabled waste separation" to aid in recycling and "use data to improve public services"—in other words, a cutting-edge "wired" development with multiple IoT applications. See Brian Barth, "The fight against Google's smart city," Washington Post (August 8, 2018). But activists pushed back, seeking information about who would control the data generated by the enterprise, and what would be done with it. The activists objected to "public" data being harvested for private corporate purposes, and argued that "surveillance capitalism" should not be the norm, ultimately obtaining a victory when the municipality negotiated a second, more government-friendly agreement with the private business enterprise. We may expect public-private smart city partnerships to engender similar reactions in other locales.

The risk of catastrophic liability is another issue that smart cities bring to the forefront. When the integrity of physical-world objects comes to depend on software, there is an increased risk that software failures will cause real-world injuries to property and persons, potentially in large numbers. One commentator has posited the specter of a "cyber Love Canal" in which buildings or entire neighborhoods are rendered "uninhabitable" for extended periods of time (as might occur, for instance, if a software bug were to shut down heating systems in the midst of a winter freeze, resulting in burst pipes and flooding). See Sean Smith, The Internet of Risky Things: Trusting the Devices that Surround Us 2-4 (2017)). The possibility of small bugs causing massive harm is, again, more than hypothetical—a massive power outage in 2003, caused when a software bug disabled a critical power grid alarm resulting in a cascading failure, ended up costing a total of $4 billion

The scenarios for personal injury and property damage in a "smart cities" setting are legion. Failure of sensors designed to protect infrastructure could result in the collapse of a building or a bridge (or a dam). Badly designed traffic systems or ancillary software could result in automobile accidents. Power outages may render homes uninhabitable, or worse. Sadly, hostile actors have come to view such vulnerabilities as an opportunity to wreak havoc, such that smart cities need to protect not only against accidental casualties, but volitional cyberharms as well. See Arthur House, "We'd be crippled by a cyberattack on our utilities," Washington Post (October 14, 2018). And even where harms seem to result from an "Act of God," the involvement of IoT systems may yield claims that the harms could have been prevented or mitigated had the systems been better designed. For all these reasons, the advent of smart cities presages a whole new era of tort litigation at the intersection of products liability and municipal liability.

In recognition of the novel risks arising from the new technologies and relationships in the burgeoning smart cities marketplace, investors and businesses considering participation in the market can and should take measures to protect themselves to the extent possible in connection with issues concerning data ownership/use and potential casualties/liability, among others. With respect to data use and rights, an initial decision is whether the data generated from smart cities initiatives is integral to the business model, or merely a byproduct. If the former, then negotiated terms must provide clarity about the business' rights to collect and use the data, while also ensuring conformance with applicable privacy and security regulations (which are increasingly stringent, viz. the European General Data Protection Regulation). Otherwise, protections need to be in place to prevent the company from inadvertent entanglement in privacy/security issues. With respect to potential casualty events, businesses should, where possible, seek robust indemnification provisions to protect themselves from the sort of "public liability" tort scenarios that government entities may face, and should consider dispute resolution provisions that would protect against "hometown" bias in the event the relationship with the government entity goes awry. It is also important to ensure that insurance coverage is available, with a sufficiently broad scope and high policy limits, to respond to casualty events that may not be subject to indemnification. In general, businesses involved in these ventures should be aware of and sensitive to the "public" dimension of these sorts of projects, from not only the legal standpoint but also the political and public relations perspectives.

Mark Raffman, *a partner in the Washington, D.C. office of Goodwin, practices in litigation, products liability and mass torts, class actions and a range of other areas.*