Smart Cities Promise Efficiency But Promote Surveillance Capitalism

The more data collected by Smart City technology the greater the risk of it all ending up in the hands of hackers. Lack of security is an existential threat to city inhabitants but only a slight nuisance to Big Tech. *TN Editor*

More than a million New Yorkers could soon willingly agree to carry a government-issued tracking device, whether they realize it or not.

That's the proposal from Mayor Bill de Blasio, who having recently returned from the cornfield-dotted campaign trail in Iowa, is setting his sights on transforming New York City into something out of a dystopian sci-fi novel. But some critics are urging caution about the move.

The fuss is about a tiny RFID chip that the mayor wants to embed into each and every municipal ID card for New York residents as part of the "IDNYC" program.

The latest proposal might seem modest, but the reality is that it potentially puts hundreds of thousands of us at greater risk of identity theft, stalking, and (for undocumented New Yorkers) deportation. And sadly it's part of the global trend towards so-called "smart cities"—a series of high-tech undertakings that claim to improve municipal efficiency at the modest price of stripping us of our privacy and autonomy.

It'd be a dubious trade-off if the technology delivered, but increasingly we see that these systems take more than we feared while delivering far less than we were promised.

Smart cities proponents claim that by integrating the internet of things, artificial intelligence, and networks of sensors that we can make our children smarter, our commutes faster, and even save lives. The outlandish claims don't end there. Smart cities are heralded as the solution to everything from the opioid crisis to de facto school segregation. Perhaps the most outlandish claim yet is that knock-off RoboCops will even prevent crimes before they even happen.

The movement is only in its infancy, but smart city programs already include every municipal service from schools, to hospitals, to sanitation, to law enforcement. And those outside major cities aren't exempt either. Increasingly, towns big and small are being taken in by the promise of a data-driven society.

MORE DATA, MORE PROBLEMS

The privacy risk is hard to overstate. Government agencies will have increasing amounts of extremely sensitive data about our health, our children's school performance, and where we spend our free time. Go to the bar? The smart city knows. Go to a protest? It probably knows that too. And so will anyone who hacks in.

Hacking isn't some theoretical risk, it's already happened. As early as

2014, security researchers starting raising the alarm that critical city systems were unencrypted and completely vulnerable to attack. That same year, the Department of Homeland Security admitted that hackers had broken into a public utility by simply guessing the password.

More recently, we've seen entire cities held hostage by hackers. Both Baltimore and Atlanta saw large swaths of their governments grind to a halt when attackers used ransomware to encrypt government computer systems, demanding a large payment in exchange for the key. Residents lost access to everything from online bill payments, to deed transfers and even court scheduling. In the case of Baltimore, not only was the city out of action for weeks by the attack, but crucial data was permanently lost.

Disturbingly for those whose health and financial data is held in these systems, hackers can just as easily post what they find in public. As *The Wall Street Journal* recently noted: "The more connected a city is, the more vulnerable it is to cyberattacks." Even with the best security protections, cities can't eliminate the threat—not as long as we continue to collect the data.

Sadly, for many smart city projects, privacy protections are not just an unwanted expense, but an existential threat. After all, even though these systems are sold with the promise of promoting government efficiency, the true product is often the public itself and all our data. Ventures like Firefly and LinkNYC use public location data to do what so many tech ventures have done: better target their ads. Smart cities create a captive, highly segmented audience ready to be told what they need to buy.

Read full story here…