

Understanding The Dangers Of Innovation Zones And Smart Cities

[Understanding The Dangers Of Innovation Zones And Smart Cities](#)

by [Derrick Broze](#), [The Last American Vagabond](#)

February 17, 2021

Following the news that Nevada Governor Steve Sisolak plans to launch so-called “Innovation Zones” where tech companies can create their own cities and governments, privacy advocates are responding with fear and concern.

During his [State of the State address](#) in mid-January, Nevada Governor Steve Sisolak noted that the state is suffering because of the COVID-19 restrictions and the effect on tourism. Sisolak called on the launch of “Innovation Zones”, a plan aimed at bringing companies working on “groundbreaking technologies” to Nevada and turning the state into the “epicenter of this emerging industry and creating the high paying jobs and revenue that go with it.” However, in these Innovation Zones, corporations are given the power to collect taxes, and essentially, operate as a quasi-independent government.

While the full plan for the Innovation Zones has yet to be released, [The Las Vegas Review-Journal](#) [obtained a draft copy](#) of proposed legislation which would grant tech corporations previously unheard of powers within the jurisdiction of these zones. The draft of the legislation states that traditional local governments are “inadequate alone to provide the flexibility and resources conducive to

*making the State a leader in attracting and retaining new forms and types of businesses and fostering economic development in emerging technologies and innovative industries.” In response, the draft calls for an **“alternative form of local government”**.*

This “alternative form of local government” will be built around the use of innovative technologies, including:

- Blockchain
- Autonomous technology
- Internet of Things
- Robotics
- Artificial intelligence
- Wireless technology
- Biometrics
- Renewable resources

While the zones would at first operate under the authority of the county in which they are located, the legislation describes how tech companies could use Innovation Zones to form their own separate government that would act as the equivalent to a county authority. These zones would have the ability to impose taxes, form school districts and local court systems, and provide government services. The zone would have a board of supervisors with the same powers as a board of county commissioners.

During his State of the State address, Sisolak noted that Blockchains, LLC was committed to developing a “smart city” east of Reno which would run on blockchain technology. [Blockchain technology](#) is essentially a digital ledger that cannot be altered. The concept was first popularized because of Bitcoin and cryptocurrency. Digital tech experts have been predicting for years that blockchain technology would revolutionize our world by integrating with various industries. Some blockchain enthusiasts believe the technology could remove the need for centralized institutions,

like banks and governments. Others worry that the use of blockchain will lead to a future where every interaction is logged on a public blockchain.

Blockchains CEO Jeffrey Berns has been promoting his vision of a blockchain smart city since 2018, when the company purchased 67,000 acres of land in the Tahoe Reno Industrial Center, which also houses Google and Tesla. Berns first revealed his plans for the blockchain city in November 2018 at the Prague Blockchain Week event.

“Imagine a world where anybody, anywhere can collaborate, establish the rules of that collaboration, enforce those rules, exchange value, and do it all on the blockchain,” Berns [said during his talk](#). *“No government. No bank. No corporation. Just trusting in math.”*

While Berns claims to be concerned with the growth of Big Tech companies and aims to use blockchain to eliminate the need for banks, corporations, or governments – ideas which are popular among libertarians and crypto-anarchists – his company also describes a vision where all life is placed on the blockchain. The Blockchains [website](#) describes how smart devices could be connected to a blockchain:

“By connecting smart devices to a blockchain – from smartphones and computers to internet-enabled cars, smart locks, advanced manufacturing machines, and security systems – we can facilitate marketplaces, payment services, or even a sharing economy for the Internet of Things. This makes possible not just peer-to-peer transactions, but even machine-to-machine payments for services, from tollbooth payments to battery storage, consumption, and trading. Best of all, because these interactions are on a blockchain, they will not rely on financial intermediaries or be subject to the security risks inherent in centralized data storage systems.”

Of course, blockchains are a tool. As with any tool their purpose is defined by the person wielding or creating the tool. A blockchain can be created with privacy, transparency, and speed in mind. Additionally, a developer could create a blockchain where every interaction is stored and publicly available for any company, government, or individual to see. What matters is how the technology is applied. Berns may care about privacy and have a desire to eliminate centralized authorities, but not all blockchains are equal and it seems inevitable that less savory actors will come along and attempt to use blockchain, Innovation Zones, and “smart cities” for the purposes of monitoring and controlling the population within the city.

For example, [it has been reported](#) that the infamous Bill Gates and his investment firm Belmont Partners purchased a 25,000-acre plot of land near Arizona for \$80 million. Gates and Belmont Partners plan to built a smart city named “Belmont”. Details on what exactly will take place within Belmont are scarce, but Gates has said he intends to grow the population to nearly 200,000 people in the coming years. However, based on Gates’ role in the [COVID-19 operation](#), his plans to control farmland, block out the sun, genetically engineer the food supply, and [vaccinate the world](#), it seems unlikely that Belmont will be a place that values privacy and individual liberty.

The Danger of Smart Cities and the Lack of Privacy Protections

The smart city trend is apparently rising as more corporations and local governments are seeking to partner together in various types of special economic or innovation zones. India has [pledged to build](#) 100 smart cities, Africa is seeing [\\$100 billion pumped into](#) at least 20 projects, and China reportedly has as many as 500 of its own smart city pilots. Saudi Arabia has also jumped into the fray with [Neom](#), a \$500 billion project that could one day rival Silicon Valley. The city will

be larger than New York City and is being promoted as the center for [“the next era of human progress”](#).

Clearly, smart cities are not going away. However, what is often not mentioned is that these smart, autonomous cities also involve massive invasions of privacy, and in some cases, giving up the right to drive or own a vehicle.

One current example of a so-called “smart city” is the Songdo International Business District (Songdo IBD), a 1,500 acre stretch of land along the Incheon waterfront, just 20 miles southwest of Seoul, South Korea. The project was built from the ground up on reclaimed land at a cost of about \$35 million. The Guardian previously described Songdo as, *“a place where the garbage is automatically sucked away through underground pipes, where lampposts are always watching you, and where your apartment block knows to send the elevator down to greet you when it detects the arrival of your car. Sensors in every street track traffic flow and send alerts to your phone when it’s going to snow, while you can monitor the children’s playground on TV from the comfort of your sofa.”*



Figure 8 Active crime prevention monitoring

Songdo was designed not simply as a smart city, but a “ubiquitous city”, a smart city with “ubiquitous” technology. A city where computers and sensors are built into the buildings and streets, sensors are gathering information on daily life, traffic, and energy consumption. As [WorldCrunch described](#) it, “In Songdo, everything has a “U” in front of it: U-traffic, U-safety, U-governance, U-health, and of course U-entertainment. The “U” stands for “ubiquitous,” omnipresent. In other words: Big Brother is here.”

According to the [“International Case Studies of Smart Cities: Songdo, Republic of Korea”](#), Songdo offers a number of safety and environmental measures to make life safer and more sustainable. However, there is no mention of privacy protections or the implications of having a living city that is connected to the grid and listening to it’s citizens on a daily basis. The report states that, “Songdo U-City collects 24-hour real-time data from on-site equipment such as CCTV, various sensor devices, traffic detectors.”



Figure 7 Vehicle Monitoring for Crime Prevention

Additionally, there is a central command center where all *“footage from crime prevention, disaster prevention, environment, and traffic surveillance cameras”* is monitored to provide useful information to the citizens. Internet of Things sensors installed in houses and building are also designed to provide *“real-time information to users, of how much energy has been consumed and what measures can be taken to minimize utility bill.”* The plan for Songdo also envisions a driverless city where residents use ride sharing services like [SOCAR](#) exclusively.

Again, there is no mention of privacy or data protections for the residents of Songdo. However, we already have examples of how a lack of privacy protections can be disastrous for residents of Smart Cities.

Quayside is a planned smart city that has been in the works since 2016. Located on 12 acres of waterfront property southeast of downtown Toronto, Canada, Quayside represents a joint effort by the Canadian government agency, Waterfront Toronto, and Sidewalk Labs, which is owned by Google’s parent company Alphabet. Sidewalk Labs claims Quayside will solve traffic congestion, rising home prices and environmental pollution. Unfortunately, residents of Quayside will be using a centralized identity management system through which they access public services, such as library cards and health care. This means their data will be highly centralized, leaving it open to access by hackers and law enforcement. In fact, Quayside has consistently faced pushback due to a failure to build-in the necessary privacy protections.

At least two officials involved in the project have resigned. Saadia Muzaffar [resigned from Waterfront Toronto](#) in protest after the board showed *“apathy and a lack of leadership regarding shaky public trust.”* In October 2018, Ann Cavoukian, one of Canada’s leading privacy experts and Ontario’s former privacy commissioner, also [resigned from the project](#). Cavoukian was brought on by Sidewalk Toronto as a

consultant to help install a “privacy by design” framework. She was initially told that all data collected from residents would be deleted and rendered unidentifiable. She later learned that third parties would have access to identifiable information gathered at Quayside.

“I imagined us creating a Smart City of Privacy, as opposed to a Smart City of Surveillance,” she [wrote](#) in her resignation letter. “I have to resign because you committed to embedding privacy by design into every aspect of your operation.”

The fears around Quayside grew in late October 2019, when [The Globe and Mail reported](#) that previously unseen documents from Sidewalk Labs detailed how people living in a Sidewalk community would interact with and have access to the space around them. This experience in the proposed smart city largely depends on how much data you’re willing to share, which could be used to reward or punish people for their behavior.

Although the document – known internally as the [“yellow book”](#) – was designed as a pitch book for the company and predates Sidewalk’s formal agreements with the City of Toronto, it does provide a vision of what the Google sister company would like to do. Specifically, the document details how Sidewalk will require tax and financing authority to finance and provide services, including the ability to *“impose, capture and reinvest property taxes.”* The company would also create and control its public services, including charter schools, special transit systems and a private road infrastructure.

The document also describes reputation-based tools that sound disturbingly similar to the social credit system we have seen in TV shows like [Black Mirror](#) and [those unfolding in modern China](#). These tools would lead to a *“new currency for community co-operation,”* effectively establishing a social credit system. Sidewalk could use these tools to “hold people or

businesses accountable” while rewarding good behavior with easier access to loans and public services.

In response to the document leaks, Sidewalk spokesperson Keerthana Rang said, *“The ideas contained in this 2016 internal paper represent the result of a wide-ranging brainstorming process very early in the company’s history.”*

Perhaps due in part to the push back against privacy invasions, in November 2019 Sidewalk Labs [released](#) a 482-page [Digital Innovation Appendix](#) stating that none of Quayside’s systems will incorporate facial recognition, and that Sidewalk Labs won’t sell personal information or use it for advertising. Sidewalk Labs says it will require explicit consent to share personal information with third parties.

Whether Sidewalk Labs, Blockchains LLC, Bill Gates, and others’ involved in the creation of Smart Cities will respect individual privacy remains to be seen. Regardless, the importance of these protections cannot be overstated. In April 2018, the American Civil Liberties Union released a guide detailing important questions that should be asked by city officials seeking to join the Smart City craze. The guide, [“How to Prevent Smart Cities from Turning to Surveillance Cities”](#), was written by Matt Cagle, an attorney with the American Civil Liberties Union of Northern California.

In a previous interview, Cagle told me that *“smart city technology can be a wolf in sheep’s clothing”* because *“it can be another way for the government to amass information that it may not have wanted to collect for law enforcement purposes.”*

“This technology is often going to be collected by companies that have developed it,” Cagle continued. *“So it’s really important for the city and the community to be on the same page about who’s going to own this data as we go forward with this project, who’s going to be able to sell this data, and at the end of the day are communities in control of these*

technologies.”

Smart Cities Are Only The Beginning

In early February, South Korean President Moon Jae-in said the government will invest \$8.8 billion into South Korea’s “smart city” project nationwide by 2025. *“The key to smart cities is to establish an intelligence-type city operation system by utilizing urban data collected from CCTVs and sensors,”* [Moon said in his speech](#) at the Smart City Integrated Operation Center of Songdo. *“First, (the government) will realize ‘smart cities’ nationwide more speedily and digitalize the public infrastructure, like roads and railways.”*

With the exporting of smart city models from Korea and recent announcements about building a smart “eco-city” in Singapore, it appears the smart city trend is not going anywhere. For the moment, these innovation zones and smart cities are simply marketing tools designed to bring people and money to the newly created cities. They are voluntary, with people freely choosing to live there and to leave if they are unhappy. However, with the understanding that the goal is to turn all cities into “smart cities”, we need to ask what happens if the smart grid is everywhere and there is nowhere to go.

In a future where all towns and cities are outfitted with the latest smart tech, fighting to maintain privacy and freedom of movement is crucial. It’s also important to understand the “innovation zones”, “special economic zones”, and “smart cities” in the context of the World Economic Forum’s [“The Great Reset”](#) vision. *How do these emerging technologies and concepts play a role in fomenting the centralized, authoritarian vision imagined by the talking heads at the WEF?*

In my next investigation I will further illustrate how the push for Smart Cities is directly related to Klaus Schwab, Bill Gates, and the push towards a Great Reset.

Derrick Broze, a staff writer for *The Last American Vagabond*, is a journalist, author, public speaker, and activist. He is the co-host of *Free Thinker Radio* on 90.1 Houston, as well as the founder of *The Conscious Resistance Network* & *The Houston Free Thinkers*.

[Connect with Derrick Broze and support the work of The Last American Vagabond](#)

cover image credit [Tumisu](#) / pixabay