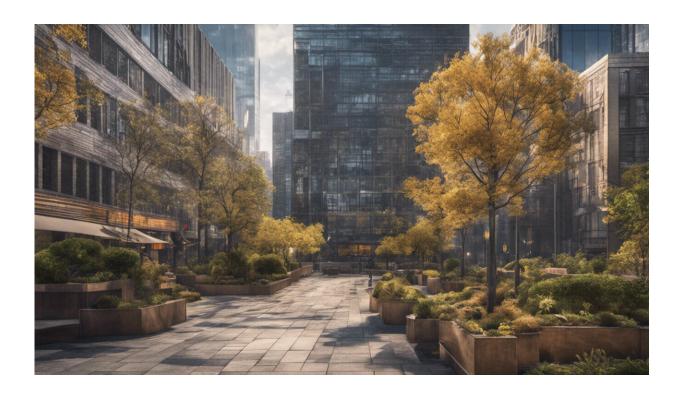# One ring to rule them all: Surveillance 'smart' tech won't make Canadian cities safer

January 22 2020, by Bonnie Stewart

Credit: AI-generated image (disclaimer)

Last fall, Drew Dilkens, the mayor of Windsor, Ont., set out to make the city the first Canadian urban center to connect to the Amazon Ring network, which the company calls "the new neighborhood watch."

Ring promises to keep more neighborhoods safe, but will smart

surveillance systems really make Canada safer? Only if the safety priority is our Amazon packages.

Ring is a suite of ["smart" home security devices from Amazon](#), based around video doorbells and an app called Neighbors. The system allows Ring customers to post and view footage from their front doors and report suspicious activity.

Customers pay monthly fees to be part of the security network. They can also purchase connected indoor security systems, [smart lighting](#) and [an integration with Amazon's Alexa](#), a smart-home device.

Framed as a way to crack down on "[porch pirates](#)" stealing packages from doorsteps, the Ring system not only makes money for Amazon, it —conveniently—[saves the company from losses](#) on stolen deliveries. Amazon's "Key" feature even allows smart system users [to grant remote keyless entry to their homes, garages or cars](#) to Amazon delivery drivers, so no package need ever go astray.

Amazon's all-seeing eye of passwords, access and surveillance infiltrating into communities is not solely a corporate system; it is increasingly connected to civic power. At the annual CES (formerly Consumer Electronic Show) conference in 2020, Amazon announced that [at least 400 police departments in the United States](#) had partnered with Amazon Ring in the previous year.

When a crime is reported, police can ask for footage from Ring homes within a radius, bypassing warrants if Ring owners comply. At least one law enforcement agency, Florida's Lakeland Police department, [appears to have been contractually obliged](#) to promote doorbells as a result of the partnership.

What does this mean for citizens and safety?

Beyond the company's own [cheery anecdotes](#), there is minimal data [proving Ring's effectiveness](#). There is [one positive 2016 report from Los Angeles](#) that predates Amazon's acquisition of Ring; the methodology of that report has not been made public.

Still, as the pioneering urbanist [Jane Jacobs](#) —or anyone from a small town —could tell you, additional [eyes on a street](#) *can* serve to deter crime.

Your uncle Bob peering out the window, however, is not the same as Ring. Actually knowing and looking out for your neighbors is not the same as a surveillance network. Ring represents an emerging governance system that, once established, we can neither vote for nor pull the curtains against. Framing Ring as a simple safety app fails to paint an accurate picture of the dangers of a makeshift corporate surveillance infrastructure.

People may assume there's no risk to them, so long as [they have nothing to hide](#). Regardless, surveillance of this kind still creates risks. At the societal level, [the ocean of datafication](#) created by pervasive smart technologies blurs the boundaries between [financial, consumer and governmental systems](#). The datafication of our personal information ultimately reduces citizens to a collection of data points, open to misinterpretation, manipulation and [monetization](#).

Do we want a societal surveillance system where public crime data is owned by a corporate entity? Amazon's interests are in profits and prevention of package loss, not in protecting citizen rights.

All smart systems create safety risks, not only of criminals hacking in but [also for customers](#). [Recent news](#) has been full of stories of [smart tech](#) and [Amazon security lapses](#), including a hacker who accessed the camera and speaker of a Ring security system in the bedroom of an eight-year-

old Mississippi girl and told her he was Santa Claus.

In addition to hacking, user data leaks are becoming commonplace with cybersecurity systems. Notably, Ring's December 2019 leak of thousands of customer passwords was denied by the company.

More safety or more problems?

Amazon has indicated —publicly and in leaked documents —that it's interested in building out the facial recognition possibilities of Ring. According to documents reviewed by the *Intercept*, the system would notify Ring owners any time an established "suspicious person" appeared on their property.

Some citizens would bear the brunt of that perceived risk more than others. Along with Ring, companies like NextDoor and Citizen show that fear-based neighborhood social media is already on the rise. Notifications about so-called suspicious persons feed race and class biases and encourage vigilante behaviors.

And even minor misdemeanors like egging cars can seem like a reason to call the police if there's video on hand.

Worse, facial recognition technology is particularly poor at correctly identifying the faces of women and people of color. Innocent brown and Black community members stand to be mistakenly harassed and even hurt.

U.S. Sen. Edward J. Markey wrote an open letter to Amazon in September 2019, expressing concerned that Ring facial recognition has serious potential to "catalyze racial profiling and harm people of color." As Canadian cities grapple with racism, classism and discrimination, tools like Ring will only undermine efforts towards breaking down bias.

In the long run, we all stand to be harmed by the happenstance creation of an integrated police-Ring surveillance network. The smart tech promise gets safety backwards. Civil and civic rights matter, and we shouldn't abandon Canada's stringent police surveillance regulations for a shiny new version of property security. A society where people are less important than packages is no society at all.

Windsor—and Canada—would be wise to say "no" to Amazon Ring.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation