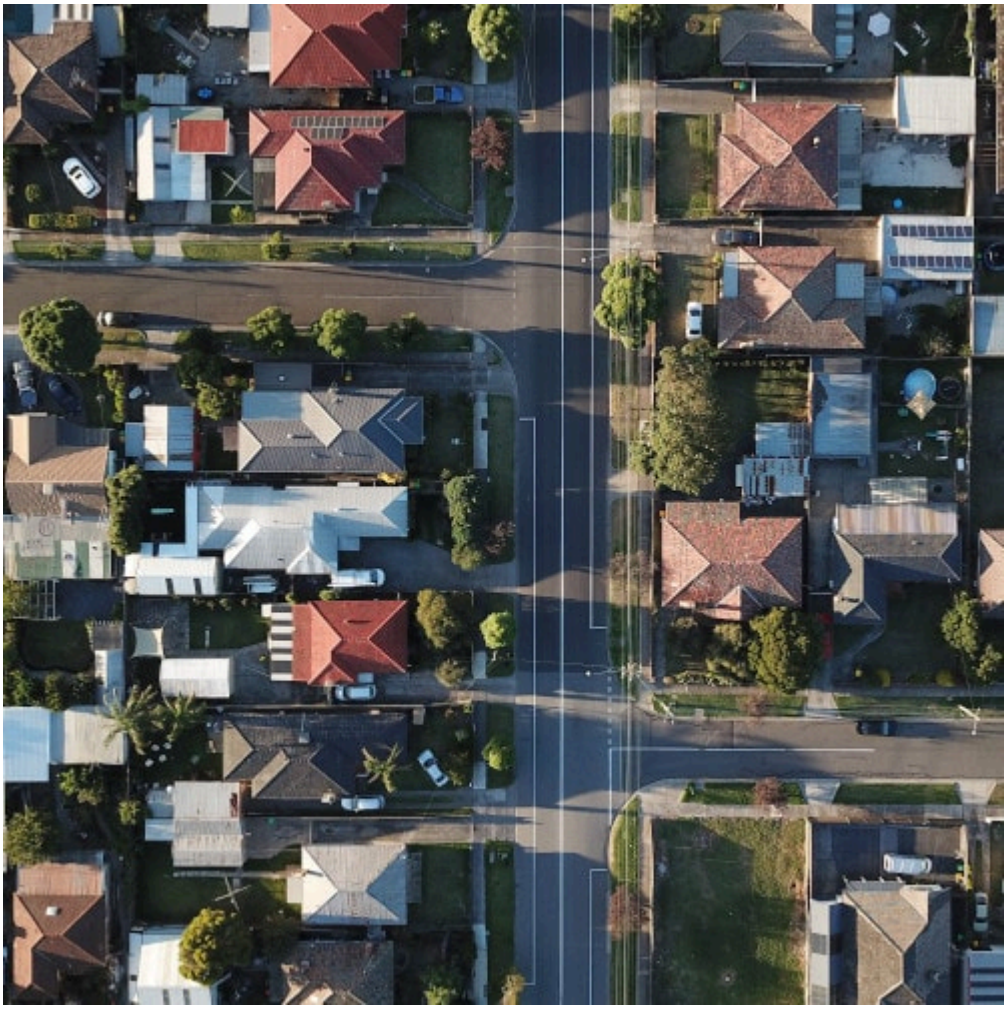
Amazon Sidewalk Needs our Trust for its Security

written by S.A. Applin
July, 2021



On June 8, 2021, Amazon deployed an “opt-in” way for people to enable the company to expand its private network into communities, creating infrastructure to peddle even more devices and services in the future. These steps from Amazon, with the cooperation of its customers, could dramatically change the way we behave in our neighbourhoods, as we are joined by more surveillance, tracking, and noisy devices that extend beyond the walls of our homes, and borders of our yards, to a near half-mile range away from them.

Background

For years, Amazon has grown, from peddling books to becoming a behemoth in retail durable goods, and, through its AWS back-end technology, a necessary component for many internet businesses and services. Amazon has crept into many homes via its Alexa smart-agent voice-controlled software. Alexa controls Amazon's "Echo" line of home-speakers that play music, retrieve information, and perform other functions. Amazon has gained a large customer following with its "Ring" video-recording home doorbell and other home surveillance and security products. These had so far been confined to the home. With "Sidewalk", Amazon now offers a service that expands the range of people's Amazon devices and services outside the walls of their homes by extending people's network capacity through cooperative sharing. Each home gives up a part of their network bandwidth to Amazon, which uses it to create a neighbourhood network. This enables Amazon's hardware to function in backyards and on the street—beyond the private environment, outside, to be utilized in newer, unforeseen ways.

> *Each home gives up a part of their network bandwidth to Amazon, which uses it to create a neighbourhood network.*

Amazon's announcement indicates more surveillance and less privacy in the Commons. The Sidewalk service offers a way for people to connect Amazon devices outside of their residences, using fractions of their and their neighbours' wireless networks. Sidewalk works with Echo as well as with Tile and Level, two types of Internet-of-Things (IoT) "tracking" discs that can be attached to pets or items to locate them. Sidewalk takes advantage of the goodwill of people and their neighbours to provide shared "mesh" connectivity outside of the home. Amazon refers to this as a "crowdsourced community benefit," but there is reason to be suspicious. Will this benefit the 'community', or Amazon? Even if someone thinks the best of Amazon's intentions, Sidewalk may affect the way we interact within our local neighbourhood community—even if we aren't Amazon customers.

Borrowing a “Cup of Bandwidth”

To introduce new products and capabilities that connect consumer data functions inside the house, to the community outside of the house, Amazon needs more bandwidth. This is acquired either by leveraging a consumer’s mobile device, or by using private internet bandwidth. Sidewalk works with Amazon devices that contain so-called Sidewalk Bridges, which includes most Echo devices and some outdoor floodlights and surveillance cameras. Sidewalk uses “Bluetooth, the 900 MHz spectrum and other frequencies” to create a private mesh-network between a household’s Sidewalk Bridges and its neighbors, with the idea that if a network goes down, or needs more bandwidth, it can use shared low-bandwidth from other households with Amazon devices that contain Sidewalk Bridges as well. For Sidewalk to work, consumers will be footing, however minor to each person, the cost of the network access that Amazon needs. Amazon claims that the “total monthly data used by Sidewalk, per account, is capped at 500MB” and adds that this is “equivalent to streaming about 10 minutes of high definition video.”

> *Will this benefit the ‘community’, or Amazon?*

But Amazon needs people in neighborhoods to agree to crowdsource their bandwidth (i.e.: free to Amazon) to enable these products, so Amazon has made Sidewalk an automatic “opt-in”: it is turned on automatically for Amazon customers who have compatible devices, rather than each customer selecting whether or not they want it in the first place. The advantage for Amazon is that the shared network is available immediately, and instantly builds their infrastructure, rather than Amazon having to wait for those who participate to “opt-in” and leave Sidewalk start off patchy and spotty. To opt-out, people will have to *tell* Amazon—and preference controls can be hard to find on Amazon’s website.

Amazon acts as if people will be willing to share a fragment of their network bandwidth with their neighbours in order to extend and increase their own network range. Ostensibly, one could install security devices more remotely on

property, or potentially anywhere in the Commons, on the actual sidewalk or in shared community space—up to a half mile away—as long as the Sidewalk network was available.

> *Amazon has made Sidewalk an automatic "opt-in": it is turned on automatically.*

Co-opting the Sidewalk

Amazon chose a name that evokes communal connectivity. It isn't Amazon "Backyard" or Amazon "Outside," it is Amazon Sidewalk. The sidewalk is physical pavement that is owned collectively by the Commons and offers us, through shared investment, a way to move through neighbourhoods and access each other's homes as well as retail environments. Sidewalks are a pedestrian space. They also function as barrier between people and cars, and a place where children play. Sidewalks imply walking, and pedestrian mobility. They're how we get around. Sidewalks provide municipal connectivity, too, in that they are akin to networks. Amazon, a private for-profit company, naming their low-bandwidth network project in this way suggests that the service is intended to extend beyond personal driveways and backyards—especially with that half-a-mile range. Along this "Sidewalk", we move along, from one low-fi mesh-network to the next low-fi mesh-network that enable our Amazon devices. It seems a kludge, but it also allows for a type of "roaming" that Amazon can wholly control, as long as there is sufficient bandwidth in the form of crowdsourced community cooperation in the form of Amazon customers who choose to participate, each forfeiting even a small amount of their paid-for network bandwidth to Amazon.

> *Amazon chose a name that evokes communal connectivity. It isn't Amazon "Backyard" or Amazon "Outside," it is Amazon Sidewalk.*

Amazon mentions further "unique benefits", such as supporting other "Sidewalk

devices" in the community, and suggests that future developments of "new low-bandwidth devices that can run on or benefit from Sidewalk" such as "pet tracking," which has been seemingly 'rebranded' and extended to the elderly with dementia, and other offerings that may use location-tracking capabilities. In its advertising, Amazon mentions that Sidewalk could help with "appliance and tool diagnostics," too, which could provide a foothold for Amazon to learn about people's appliances—and how we use them.

People's readiness to offer their bandwidth to enable these products in a way shifts the development of Amazon products that reach beyond the home and into the Commons onto its existing customers, making them unpaid financial backers and "creators" of a sort—by funding the network capabilities that enable Amazon's expansion, and deploying the devices that increase Amazon's reach. Customers will do this even as they pay for Amazon's services for the products they already own, such as the Ring doorbell hardware the extra for "Ring Protect Plans" that cost anywhere from US $3-$10 per month.

Expanding Amazon's Reach

Amazon encourages such a coordinated network participation to include more objects, more ways for surveillance, and more infrastructure built to process the "more" data that it is collecting—in addition to an extensive global retail empire that sells its customers just about anything. These factors, combined with Amazon's extraordinary data footprint, the ability to analyse extensive retail consumer behaviour, and long tail of relationships with the Police, make Amazon's growing Ring/Echo/Alexa surveillance apparatus have the potential to generate very real and unfortunate consequences that could impact people's lives in deep, severe, and unforeseen ways—even if unintended by Amazon.

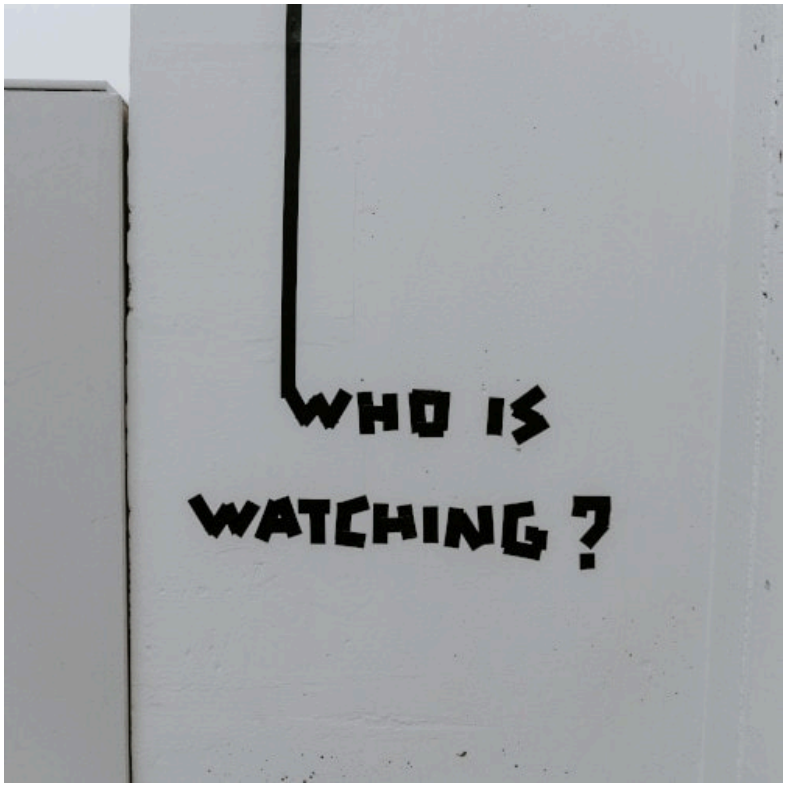


Photo by Claudio Schwarz on Unsplash

Amazon envisions us stuffing our homes with Amazon products that are tied together with Alexa—and, now, Sidewalk. It is also planning an "indoor drone" to capture in-home surveillance footage, a Ring Car Alarm, a Ring Car Cam, Mailbox Motion Sensor, and even an Alexa Guard Plus service. The latter offers "listening and watching" Smart Alerts surveillance, including ways to take action on commands that Alexa either enacts on the customer's behalf, or via command. On the back-end, these commands appear to be broken down in tiers of algorithmic triage—if someone has paid for the service.

> *Citizens purchased Ring doorbells on the advice of their local police department. Thus, public servants became an authority for advertising for Amazon.*

For example, if Alexa is set into "Away Mode", but "hears" sounds that are abnormal, such as shattering glass, footsteps, coughing, water running, or other

‘break-in’ predetermined conditional clues, Alexa will respond in a series of steps. First, it will send the customer a Smart Alert. Alexa might “increase its reaction” if the sounds are of a potential intruder—however they’ve classified these—which is potentially another problem. At that point, Alexa will “react” by playing a siren through an Echo device. If the homeowner has the outdoor motion detection option for cameras and lights, Amazon Guard Plus will work with smart cameras to turn on lights and play sounds of dogs barking to deter break-ins, too. If someone is home, the Amazon Guard Plus service includes options to call Emergency Services directly using Alexa—if the homeowner has signed up and paid for Alexa Guard Plus at $4.99/month, or $49/year. Amazon Guard Plus also offers “hands free access to an Emergency Helpline,” staffed by “trained agents who can request the dispatch of emergency responders — such as police, the fire department, or an ambulance — based on information you provide on the call”. It is unclear what credentials or training these agents would have. Amazon responded to my author’s inquiry about how these agents were trained, and what they might know: “Amazon enlists the help of a professional monitoring service to train and staff the Emergency Helpline with agents who are available 24/7, 365 days a year” (personal correspondence). This means that if this third-party service is used to broker between an Amazon customer and emergency services, there may be additional routing vs. directly calling an emergency code such as “911,” when used in the US.

Amazon is increasingly becoming an algorithmic replacement for the police, and in ways is changing how police gather information on communities. It first joined the home security market by offering Ring video doorbells that could help people monitor their properties by recording outside the home. Amazon has a huge data processing network on the back-end of their Ring doorbells and other products, which has computing power that no police department can dream of matching. Additionally, since Amazon heavily partnered with Police departments to promote Ring to citizens for “safety,” citizens purchased Ring doorbells on the advice of their local police department. Thus, public servants became an authority for advertising for Amazon.

> *Amazon's product creep pushes community boundaries into territory that is the responsibility of municipalities.*

It seems hard to imagine that Amazon is solely creating Amazon Sidewalk and other products, especially Amazon Guard Plus, as a goodwill measure to increase people's security and the robustness of Ring. Rather, it appears to be more of a business decision to build products that are both likely to sell well and increase Amazon's data cache. But from outside, it is hard to speculate about Amazon's further goals, or how its various product announcements could work together. Amazon has also announced its intent to capture video footage in and around its delivery vans by installing AI-enabled surveillance cameras that will film drivers and the public streets in front of and behind vans. Depending upon range and scope, that may inadvertently (or purposefully) include sidewalks, driveways, and front porches. Described as a way to keep package delivery safe, the data these cameras collect will be owned by Amazon.

Pushing Community Boundaries

Amazon's product creep pushes community boundaries into territory that is the responsibility of municipalities—and it is continuing to develop more and more different ways for watching, listening, and collecting neighbourhood data. With mobile surveillance, Ring, Sidewalk and potentially other devices together, Amazon is creating a surveillance enterprise by which there could be sweeping community monitoring, even if Amazon claims to be collecting "minimal data" with Sidewalk. An Amazon spokesperson wrote that Sidewalk "uses one-way hashing keys, cryptographic algorithms and rotating device IDs to minimise data tied to customers" and that "routing information … for operating the network components of Sidewalk is automatically cleared every 24 hours." But Amazon already has detail on what is inside our homes and our minds that surpasses anything a municipality could clock—and with Sidewalk, the extension of data

seems imminent. People are continuing to pay Amazon for surveillance services, and while their neighbours or passers-by become the objects of surveillance, the Amazon customers themselves could be monitored— even if they are not at home.

The worst-case scenario could be when the aggregate of the Amazon Sidewalk/Amazon Guard Plus-enabled devices are shrieking, barking, flashing lights and generally reacting to every nuanced "different" algorithmic match outside of our homes. Our neighbourhoods will change, first with Amazon Sidewalk and various sonic disruptions from their devices. Backyard Sidewalk-enabled music, commands, controls, alarms, and warnings may increase neighbourhood conflict, as people have different preferences for outdoor space, and extend their devices' ranges outside their homes. The "outsourcing" of surveillance to automated algorithms will have an impact, whether it is as mild as devices being noisy or more severe such as misdirected emergency resources. Artificial Intelligence is great at pattern-matching—if it has learned the pattern. With so many new algorithms and services being deployed simultaneously in communities, the possible range of errors across all of these, and the potential for these errors to be magnified in aggregate, is concerning.

> *We are trading our peace and quiet for the clamour of Amazon's warnings.*

More seriously, valuable community resources may need to be deployed if Amazon Guard Plus algorithms claim a break-in in progress and people call for help to stop the ongoing alarms in their neighbourhoods. These resources (paid for by taxes) may be dispatched to investigate Alexa-enabled calls more frequently than required, as algorithms (and people) learn the patterns inside (and outside) of homes. Imagine people needing Emergency Services and not being able to get access to them because the responders are busy reacting to potentially miscalculating algorithms setting off alarms. This shift to algorithmic policing (by a private company) also in part replaces the police and/or the patrols of professional security firms. Machine-learning algorithms can "listen" but cannot truly see—even with cameras. Lastly, the various permutations and surveillance

combinations that customers can create with Amazon's product line-up may also create different kinds of heterogeneity that compromise the very security it is attempting to provide. Not all people's device combinations may necessarily work in the streamlined fashion that Amazon seems to be advertising, and with such heterogeneity often comes vulnerability.

The kicker in this entire 'Amazon subsumes the Commons' product launch is that customers are paying for the whole thing: Amazon Ring and services, Amazon Guard Plus, Amazon Sidewalk network bandwidth "micro-funding", taxes for emergency responders, job forfeiture out of the community to algorithms, the list goes on. But most of all, we are paying with our way of being and we are moving our sense of social trust onto Amazon. We are trading our peace and quiet for the clamour of Amazon's warnings, we are trading our trust of each other (and perhaps in this case more rightly trust in the police) for trust in shared networks, and moving that trust to Amazon and other third parties to manage.

Featured Image by Tom Rumble on Unsplash.

This article is an expanded version of a shorter piece by S.A. Applin, which was published in Fast Company on March 31, 2021.