The Vacuum That Knew Too Much:
7,000 Robot Vacuum Spies In Our Homes!

BY **CHRISTOPHER SALGADO,** CEO OF ALL POINTS INVESTIGATIONS, LLC

One evening, a young cyber prodigy sat on the family couch alongside his trusty cat, Commander Pickles. Both the child and the cat were enamored at the family's robot vacuum, or robovac, but not for a good reason. They weren't marveling at its unmatched ability to navigate the close-quarter confines of the living room, dodging the coffee table legs, the cat tree and rabbit cage like a gold medal Olympian skier on the Slalom. They were enamored with the smart vacuum's ongoing failed attempts to, well… be smart. The robovac successfully presented the image of being anything but smart as it bumped into every obstacle like a drunken sailor on Independence Day. The disappointed stares of the child and the cat seemed to plea for an option capable of cleaning without a side of destruction.

So, the boy got to work. Instinctively, he ran towards his video game console, grabbed its controller and began adding some corrective lines of code along with convenient ones to his experiment. Alas, his video controller was successfully converted into a remote for the all-improved robovac. The kid's captivated audience – the cat – looked on as the boy relished in controlling the robovac more successfully than the vacant promise by its manufacturer.

Then, it happened.

The screen that displayed the first-person view of the robovac – hooked up by the child – didn't just show his vacuum. It showed the display of a separate and unknown robovac… and another… and another. Within a very short time, he was able to access thousands of robot vacuums around the world – in real time!

Every one of these additional robovacs reported their location, battery levels, and cleaning maps just as if they were all owned by this child. Oh yeah, and he could hear through the robovacs' microphones. – Yes, the robovacs come with microphones!

Yes, that trusty, modern marvel of machinery that spreads joy to us human folk, yet terror into the lives of small dogs, is a gateway for any tech savvy bad actor to enter your home – complete with live video and audio!

The origin of this dramatized version of an otherwise true story comes from the hands of Software Developer Sammy Edufel. According to WFAA (Dallas–Fort Worth) on Mar 1, 2026, "Software developer Sammy Edufel was building an app to hack his DJI Romo smart vacuum. He wanted to use his PlayStation controller to make it move, but in the process, he accidentally uncovered a major security flaw with the help of an AI chatbot. Sammy discovered he could also access what he says were roughly 7000 other vacuums, allowing him to get their approximate locations and even remotely control other people's vacuums. He could also see through other users' live camera feeds and hear through their vacuums' microphones…"

The above terrifying "Big Brother" 1984 scenario, historically destined for pages in a fiction book or a movie script, has been transformed into real world horror thanks to our modernized world and extreme demand for convenience and "cool" devices. Even well before the above scenario, our safety in our own homes has been challenged by offenders targeting us through the Internet of Things (IoT). – Basically, our devices connected to the internet.

From online baby monitors to smart refrigerators to smart TVs and on and on and on, we're continually placing ourselves into the risky world of digital intrusions due to our insatiable need for convenience through smart gadgets.

This reminds me of a time that I received a gift that was a smart robodog. It was innocently sent to me but after I opened the box and read the details of the robodog, I immediately boxed it back up. I was asked why I did that. I responded that I have a large concern with any device that passively listens, offers a microphone that can be hacked, maps my residence or offers a camera that can also be hacked. I felt bad for the sender of the gift, but I wanted to safeguard my home from the prospect of external intrusions. Morning news streams detail case after case of our own products spying on us – allowing us to be infiltrated by a bad actor due to some overlooked security loophole or such.

My tech life choices may not mirror yours. That's OK. In fact, maybe you have a robovac! If that's the case, what do you do?

Speaking from a remote intrusion perspective, there are only two ways that someone can infiltrate your life: via a device or via data. Therefore, you must ensure that you lock

down the digital element and the physical element of your robovac. That includes placing a piece of duct tape or electrical tape over its camera. (Physical element.) Deactivate your robovac's microphone. (Digital element.) Also deactivate your robovac from third party apps, including Alexa and Google.

You can also ensure to create strong passphrases (not passwords), activate 2FA or MFA and disable microphone and camera features. Disabling the mapping service can be beneficial as well. While the latter won't prevent an intrusion, it can limit the data available to an offender, should an intrusion occur.

The above is a good start to negate this specific attack – even an accidental one, as was the case in the above real scenario (not my dramatized version). There are additional mitigating steps that can be taken but, again, this is a good start.

I'll leave you with the reminder that our modern world can certainly be fun. It delivers extreme convenience – devoid the countless times you've invoked your rage monster before striking your phone due to significant signal loss, which was caused by a constrained network in response to thousands of like-mined giddy individuals streaming content at your attended massive comic convention. Yes, sometimes our smart devices bring out the worst in us but, many times, they provide insta-satisfaction as our butlers of global intelligence at our fingertips. I've said this before, I'm not interested in fearmongering or promoting the idea that we should avoid our connected devices. I'm simply educating you to the landscape of modern dangers. In turn, I try to offer actions that can negate or mitigate such dangers. The trillions of lines of innocuous code that reside in our software ecosystem can be reprogrammed to invert good intentions and deliver chaos into our lives. Just look at all of the online scams and cyberattacks directed against us as a global society.

It's critical to understand the dangers surfacing from our unbridled demand for ultra convenience through smart this and smart that. If we can truly understand those dangers: what they are and how to negate them, maybe we'll recognize today's modern world in the mirror, reflecting our technical ambitions. Such an awakening can help stand up proper protection for us. Then we can shift our focus to tomorrow's modern world. – That one concerns me more. **PI**

Christopher Salgado is the CEO of All Points Investigations, LLC, a global cyber and physical investigative firm serving Fortune-listed corporations, law firms, and other entities. A former Facebook investigator, he brings over 20 years of expertise in cyber investigations, OSINT, cryptocurrency, social engineering, and threat management. His work spans corporate risk, brand protection, cults, cyberstalkers, SIU matters and others. In 2024, he was named a Top Investigator by PI Magazine. *Christopher is a member of the London Speaker Bureau and a keynote speaker at industry events, including CrimeCon. He has*

briefed agencies such as the FBI, DEA, HSI, CBP, Interpol, Europol and members of the EU Commission. He is also the Founder of Anti-Hackathon, an online safety initiative, and AGGOSO™ Training, an advanced OSINT education program. He may be reached at csalgado@allpointsinv.com