Yes, China is probably watching us through our IoT devices

By Maya Shwayder
March 6, 2020

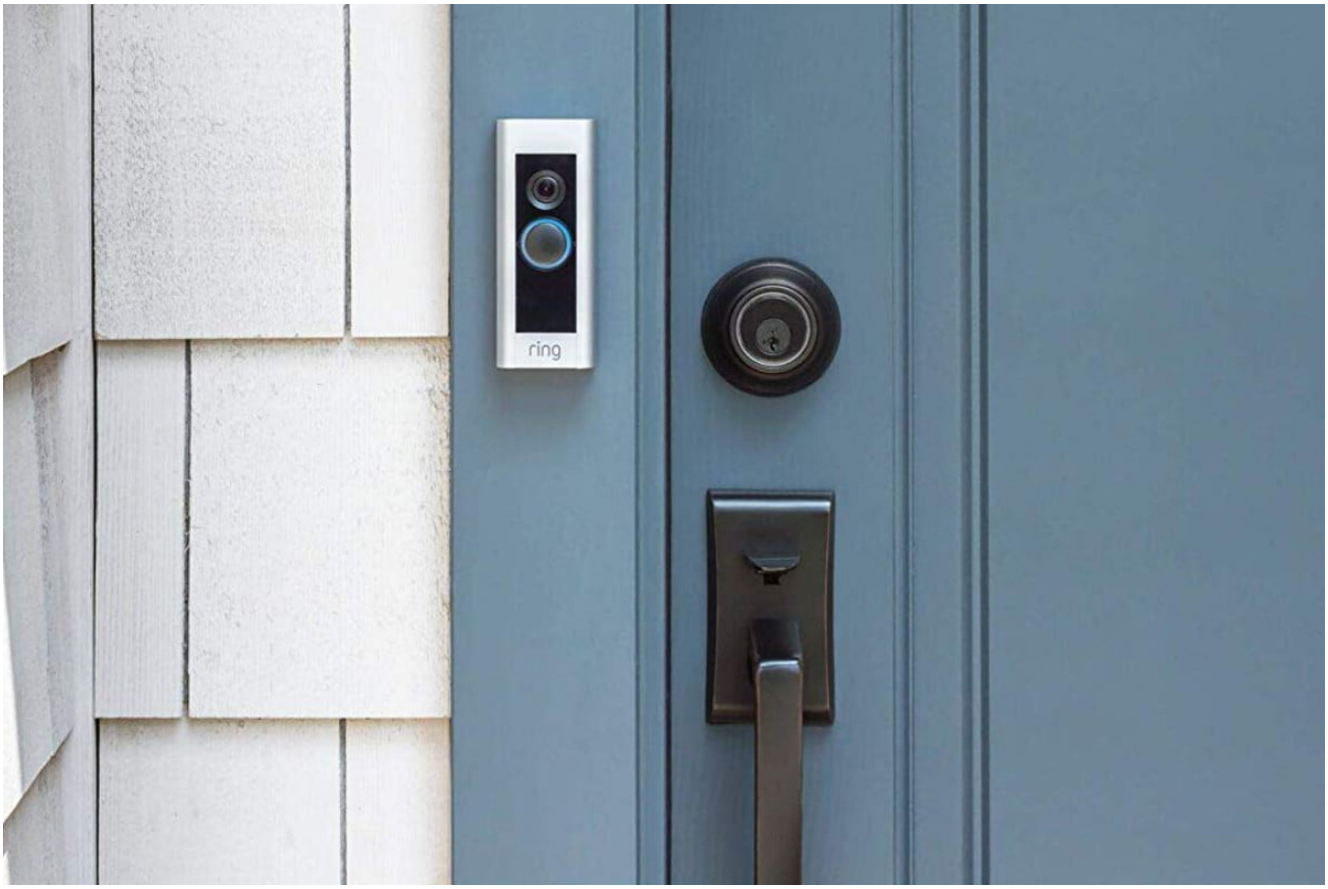
Is your phone/laptop/home security camera spying on you for the Chinese government?

Well, probably.

Should you care?

Yes… but also, how much of a choice do we all have?

Internet of Things (IoT) device security — particularly in home security camera systems like Wyze, Aqara, and Ring — has been a hot topic lately. The devices have repeatedly been shown to be leaky and insecure at best, with no two-factor authentication or encryption present. This has allowed for a multitude of incidents wherein hackers have gained control of people's digital lives and threatened them.



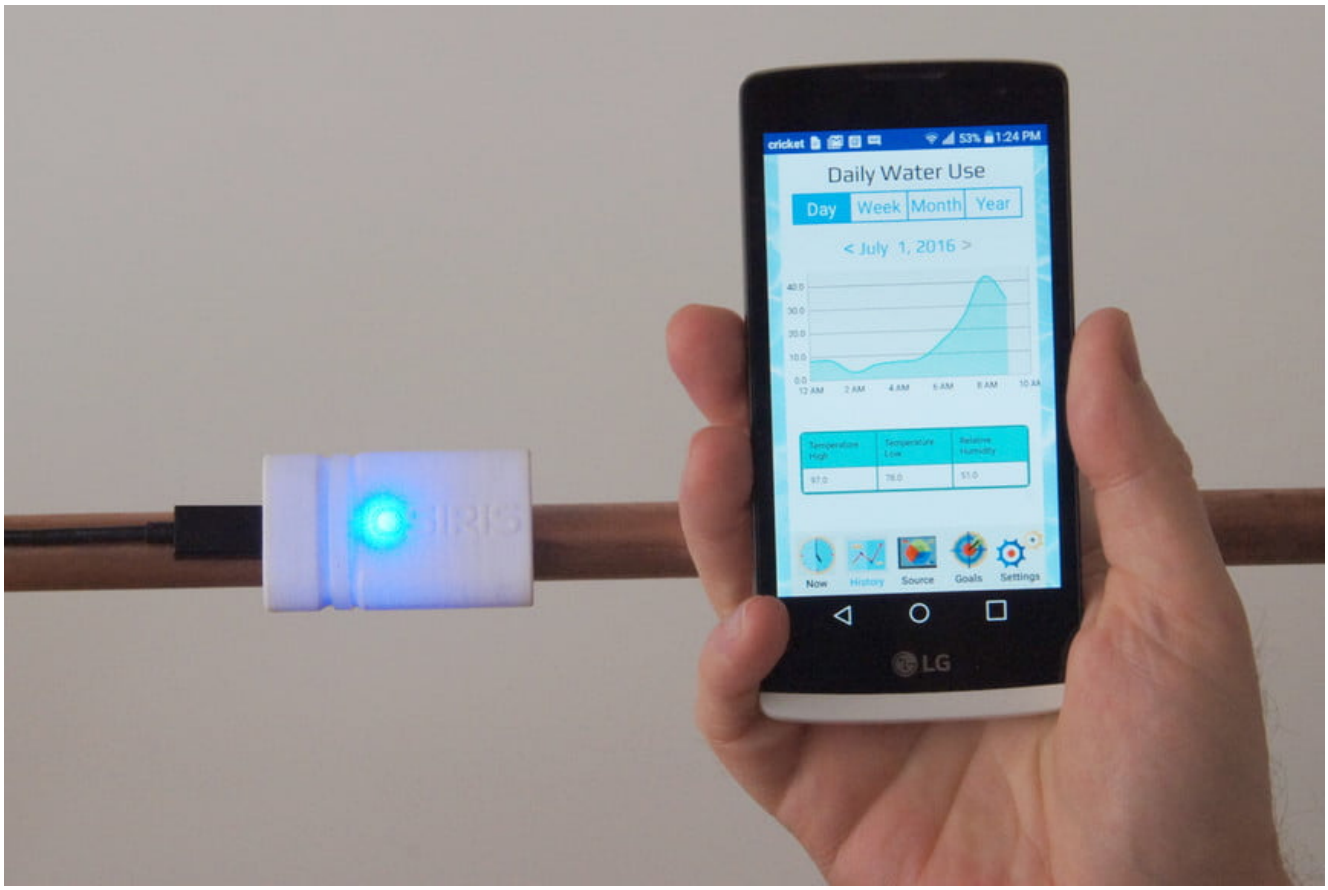
Holistic approach lacking

But a wider problem still is the passive watching that might be happening. Man of the devices are assembled in China, using Chinese parts. Even if the companies are not explicitly Chinese, this presents a threat. So much so that the U.S. Department of Interior at the end of January instituted a ban o n Chinese-made drones and drone parts over fears that the tech might be sending information back to the Chinese government.

“In general, IoT devices contain many third-party components and differen communication stacks, which provide many ways for malicious parties to hack into them,” said Natali Tshuva, CEO and co-founder of Sternum, an Israeli cybersecurity company that works on secure connectivity for IoT devices, in an email to Digital Trends.

This is changing, somewhat, Tshuva said. Common vulnerabilities in IoT systems like Elasticsearch databases being left open for access without credentials are problematic, she said. This emphasizes the need for end-to-end encryption.

“Companies are taking steps to enhance the security of their devices, but they are lacking a holistic approach that covers all security aspects of their devices, leaving an opening for attackers to exploit them,” Tshuva wrote. “Wit billions of IoT devices coming to market now and over the next few years, it’ critical that each device is embedded with security.



Price drives the bus

The problem, said Jimmy Jones, telecoms cybersecurity expert at Positive Technologies, is that these companies care most about being first to market and this means cutting costs. “Everything is driven by price point. People don’t want to pay that extra dollar,” Jones told Digital Trends. “So they [th companies] end up using third-party software and third-party parts. The problem is, a lot of [the devices] do come from China.

“It’s hard to tell what’s malicious and what’s just incompetent,” said Ron Gula, a former National Security Administration white hat hacker and current investor in cybersecurity startups. “Let’s say there are some companies that have perfec security on their devices, but they are still based in China,” he said. “All of tha data they collect, the Chinese government can ask for access to it. Or it migh even have implied access, and they don’t have to tell us about it.”

Who is China spying on then, if is indeedspying? “In a word, indirectly, probably everyone,” Jones said. “But it’s not necessarily cause for alarm; it’s a trust situation.”

So much of our lives are produced in China now. Where do we draw the line as to what products we’re willing to accept from there, Jones asked. “Is it a car? Is it a drone? Is it a light bulb? Is it a central heating system?” Jones said, pointing to two stories, one about a DDOS attack in Finland that shut down acity’s central heating system, another about smart light bulbs leaking Wi-Fi credentials.

“We’ve seen it with Huawei,” Jones said, referring to the Chinese phone manufacturing giant that has been the target of much ire from the Trump administration. “These companies, or their holding companies, are all owned by the trade unions. The Chinese Communist Party is essentially the head of the trade unions, so reall,y everyone is just two steps away from being owned by the Chinese government.”

“There has to be a point where trust needs to take precedence,” Jones said. “Or, do we create a new superpower to manufacture our stuff, and then in 10 years we decide we don’t trust them either?”

Requiring everything to be made here in the U.S. isn’t really that feasible, said Gula. “Our iPhones are built in China,” he said. “Like most Cisco routers and most laptops.” And honestly, he said, that isn’t what matters here. The bes antidote right now is just to educate the public.

“When your data’s in the Cloud, you hope it’s protected, but it’s honestly subjec to the laws of wherever it’s hosted,” he said. And then there’s a question of where the data that’s transmitted through these devices is stored. “Data provenance, and where it’s stored, and who has access is a big deal.”

“I don’t want to see ‘Made in China’ stickers,” Gula said. “I wanted to see ‘Data Hosted in China’ stickers.”