Are Your Appliances Spying On You?

These days, it's possible to use your phone — and sometimes just your voice — to control everything from your TV to your lights, your thermostat and shades, even your car or medical device.

According to the technology research firm Gartner, 8.4 billion "connected things" are in use around the world this year, up 31% from last year. That figure is expected to reach 20.4 billion by 2020.

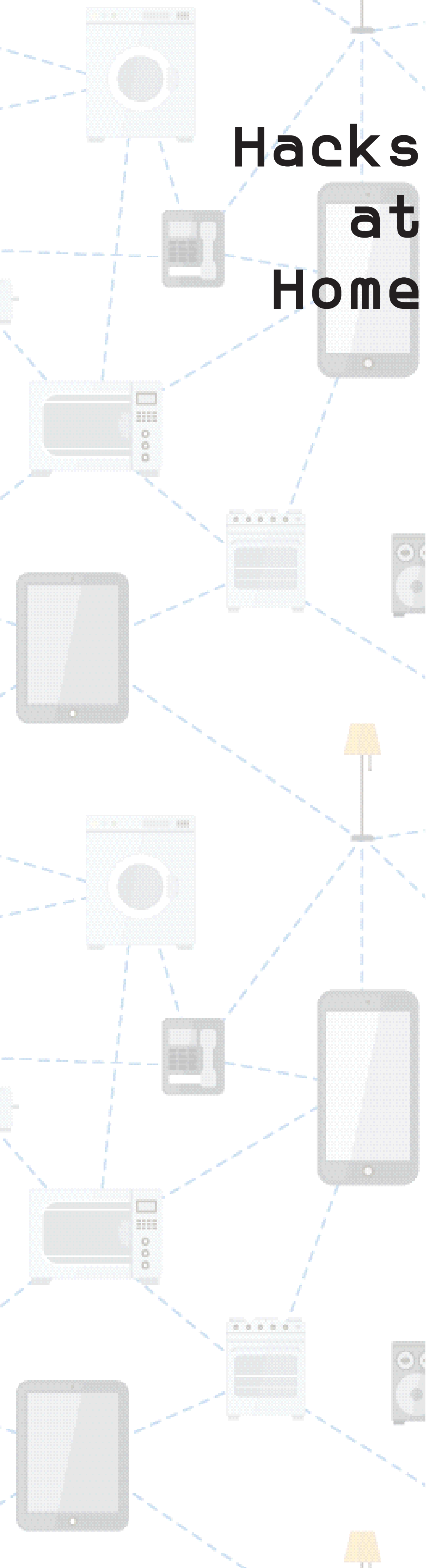
The amount of information collected by these smart devices is staggering. A Federal Trade Commission report this summer concluded that just 10,000 households can generate 150 million discrete data points every day.

What new powerful insights into your personal life will a company have when its entertainment system is in your car, its thermostat regulates the temperature in your home, and its smart watch monitors your physical activity?

Former CIA Director David Petraeus told ABC News he believes that even mundane appliances like your dishwasher could soon be used to gather intelligence about how you live.

Hackers know that and have targeted smart devices to capture personal information and make money. Consider some of the ways "smart" wireless products can put your personal information at risk.

Hacks at Home



TVs:
Last February, Vizio agreed to settle charges that it violated the law by using software in its “smart,” internet-connected TVs to collect data on what users were watching, without permission.

In 2015, Samsung drew criticism for its always-on voice detection privacy policy that stated, “Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party.”

Users can navigate the menu on many smart TVs to opt out of this practice by going to Settings > Support > Terms & Policies and opt to “Disagree” with the policies for Viewing Information Services, Voice Recognition Services, and Nuance Voice Recognition and Privacy Notices.

INSULIN PUMPS AND DEFIBRULATORS:
In 2012, a hacker named Barnaby Jack, recently deceased, proved he could kill a diabetic person from 300 feet away by ordering an insulin pump to deliver fatal doses of insulin. ABC News reports this summer, he announced he could hack pacemakers and implanted defibrillators.

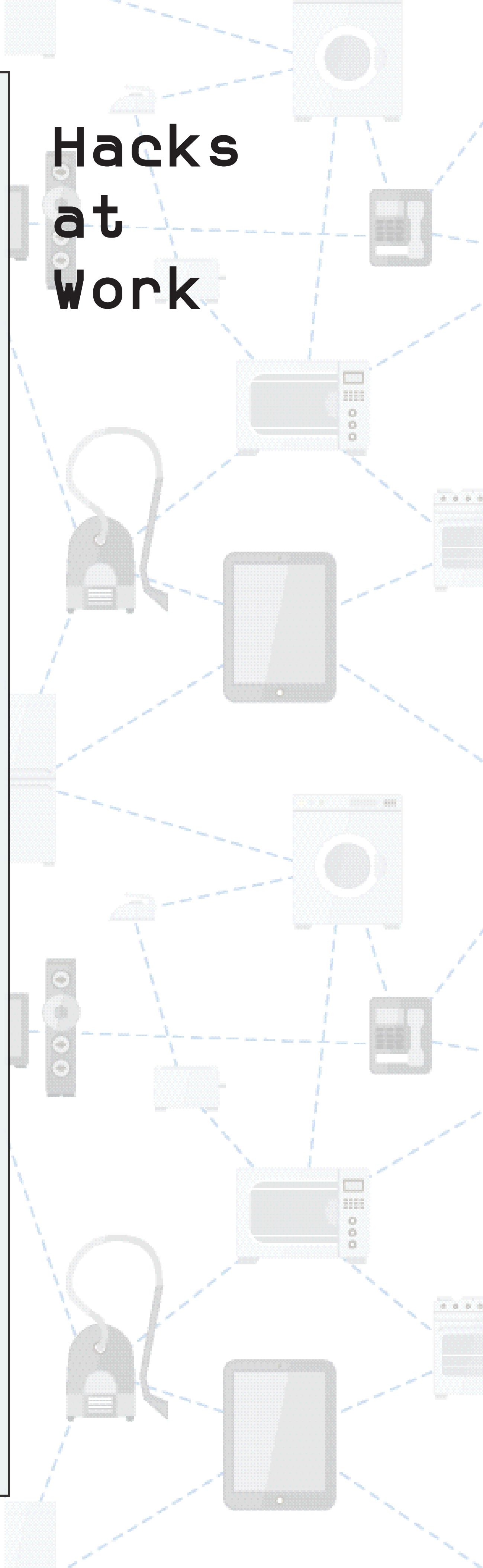
REFRIGERATORS:
Samsung sold a smart fridge that didn’t operate securely. A fraudster could hack the refrigerator to monitor the user’s wi-fi network and snag their Google login information.

TOYS:
In July, the FBI warned that fraudsters can target unprotected Bluetooth-connected toys that do not require PINs or passwords when pairing with a mobile device. Voice recordings, the passwords used with the toy’s software, home addresses, Wi-Fi information, or sensitive personal data could be exposed if the security of the data is not protected.

Spiral Toys sells internet-connected smart stuffed toys called CloudPets, which allows children and their parents to communicate via voice messages. The company reportedly left over 800,000 user accounts’ data exposed exposing over 2 million recordings of children and parents online in the days that followed last Christmas.

CABLE TV BOXES:
ABC News reports Google and Verizon are developing cable boxes with built-in video cameras and motion sensors. The purpose is to determine who is in the room watching, enabling personalized ads to be shown. If the camera detects two people canoodling on the couch, they might be delivered ads for a new romantic movie, while a roomful of children would see ads for an Air Hogs remote control helicopter.

Hacks at Work



VENDING MACHINES:
Last year, hackers took over 5,000 wireless vending machines and light sensors at an unnamed University.

Verizon says the malware instructed the likes of lights and fridges to turn their requests against the university in order to overwhelm the network.

Hackers commanded the smart devices to repeatedly look up nearby seafood restaurants, slowing the institution's entire network and restricting access to most internet services.

TEA KETTLES:
Tests at BlackBerry showed similar vulnerabilities in their office's network-connected tea kettle, which they proved could infiltrate an entire network and put sensitive company information at risk.

PRINTERS:
In February 4, 2017, a high school student in the United Kingdom sat in front of his computer and instructed 150,000 internet-connected printers across the world to spit out art and messages.

Motherboard reports many of the affected printers were connected to restaurant POS systems, leaving confused employees to find images of robots pouring out of their receipts.

There's a growing call for regulation to secure connected devices, but it's unclear whether this will happen.

Krebs on Security, a respected cyber security newsletter, says lawmakers in the U.S. Senate introduced a bill in recent weeks that would set baseline security standards for the government's purchase and use of a broad range of Internet-connected devices, including computers, routers and security cameras.

The legislation also seeks to remedy some widely-perceived shortcomings in existing cybercrime law.

But for now, it's up to buyers to protect themselves and their families when buying smart devices.

What To Do

to Keep Your Family Safe

1: Scan your house for existing wireless issues

Start by scanning your home network to make sure it isn't already infected. Newsweek recommends using this link offered by the security firm Bullguard: http://iotscanner.bullguard.com

2: Update your wi-fi password

Your Wi-Fi password shouldn't still be the one it came out of the box; it needs a hard-to-guess passphrase to ensure that it can't be easily hacked.

3: Understand the privacy policy for all the wireless products you buy

Read the privacy policy and understand what the device manufacturer can do with information it collects.

4: Never use default passwords

If a smart device comes with a default password, change the password the moment you hook it up.

5: Don't skimp when you buy

Buy trusted brands. Cheaper devices from no-name companies pose more of a security risk. While companies like Apple, Amazon or Samsung can patch up security holes as soon as they find them, smaller companies don't have the resources — or sometimes the ability or willingness — to do so.