THE TROUBLE WITH WEARABLES

Electronic gadgets on — and in — our bodies are multiplying fast, but transmitting all their data safely will be a challenge.

BY KAT AUSTEN

Tom is late for his train and doesn't know the way to the station. Racing around a corner, he runs into a plaza full of tourists snapping and uploading photos to Instagram and Facebook. Which way should he go? He tells his Internet-connected contact lenses to load a map, meanwhile tapping at his smartwatch to pull up his ticket and platform information. An alarm flashes in his peripheral vision, only 15 minutes until the train departs, but the map is not loading. He looks around in dismay, frantically yelling "refresh" to his lenses against the clamour of the street. An alert scrolls across his vision: "You're feeling stressed. Take a breath. Have a hug!" But with all the tourists accessing the Internet, Tom has no hope of getting his much-needed map.

Welcome to the chaotic future of wearable electronics: devices that promise to connect real to digital lives seamlessly. These gadgets are rapidly multiplying, and within five years there could be half a billion devices strapped onto, or even embedded in, human bodies. Today, the most familiar gadgets are fitness trackers and smart watches, which monitor health and provide ready access to online services. But there are already devices that claim to do more than monitor, such as headbands that alert wearers when they become distracted or wristbands that administer electric shocks to smokers who want help quitting. Electronics companies promise to transform medicine with wearables that can treat symptoms or manage care. Devices are emerging that alert people with epilepsy to incipient seizures, help prevent anxiety attacks, and enable blind people to navigate.

But the potential of wearables crucially depends on the large amounts of data they access and generate. And that leads to two problems that researchers and technology developers are struggling to solve: finding improved ways to transmit data to and from wearables, and keeping all that information safe. With everything from toasters to cars now connecting wirelessly to the Internet, demands on a finite bandwidth are rapidly straining the system. Nearly half a billion new devices started chattering over mobile broadband last year alone, pushing mobile traffic to 25 times what it was just 5 years ago. And wearables are leading to new security concerns, from the use of highly personal data to track people's activity to maliciously attacking their online presence.

"It's a cliché that whenever there's a new technology we start talking about Huxley and *A Brave New World*, but with wearables — and what's loosely termed the Internet of Things — we truly are entering into a new era, and we have to start thinking of these issues," says Anupam Joshi, head of the Center for Cybersecurity at the University of Maryland, Baltimore County.

TRAFFIC JAM

By the end of 2014, global mobile-data traffic reached 2.5 exabytes (2.5 billion gigabytes) per month according to the networking-technology company Cisco Systems. Of that, the world's 100 million or so wearable devices were generating 15 million gigabytes of monthly traffic on what is a physically finite portion of the electromagnetic spectrum, with their number expected to increase fivefold by 2019 (see 'The catch with gadgets'). On top of the surge in those devices, there will be even greater chances for gridlock, as more people start wearing headsets that deliver data-hungry virtual and augmented reality experiences, says Robert Heath, a professor in electrical engineering at the University of Texas at Austin.

All these devices clog up the airwaves, impairing performance and threatening essential internet traffic. To help ease congestion in the United States, the government pledged in 2010 to free up an extra 500 megaherz (MHz) within ten years, a doubling of the bandwidth available for mobile devices at the time. But even this is unlikely to be enough, according to a more recent report prepared for CTIA-The Wireless Association, a communications industry group based in Washington DC. It estimates that 350 MHz will need to be added from 2015 onwards to keep up with US demand by the end of 2019, 150 MHz more than the government estimate for that period. And limited bandwidth is a global problem, with each country dealing with it in its own way. In India, where users have access to just one-tenth of the bandwidth available to people in the United States, there are calls for spectrum sharing

and the freeing up of channels currently devoted to the military. In the United Kingdom, the government has approved the use of old analogue TV bandwidths; the first networks of smart devices using these frequencies could be rolled out by the end of the year.

For their part, telecom companies need to make more efficient use of the spectrum. One way is to look beyond the crowded parts of the airwaves in the radio and television bands. Data from all the wearables on one person could flow through a body-area network designed to use a completely different part of the spectrum, such as the millimetre wavelengths. Then just one device would use the more congested bands to communicate all the data to the Internet. This creates its own problems, however, because shorter wavelengths demand more power and can be blocked by people's bodies. So researchers such as Heath are trying to get around those difficulties by, for example, optimizing antennas to reduce interference and power consumption. Improvements in steerable communication beams could also lead to better ways of transmitting millimetre-wavelength signals.

Also promising is the idea of taking wireless communications into the visible-light realm using light-emitting dioides (LEDs) — which produce light and can act as photoreceptors — to communicate either between wearables or to talk directly to the Internet. Wearables that incorporate LEDs could use visible light to wrap a person in a body-area network. That would sense every movement and communicate the information to the light fittings in a room, which would be connected to the Internet through their power wiring. Although this technology relies on visible wavelengths, the signals are imperceptible. "LEDs blink so fast that the human eye cannot tell," says Daniele Puccinelli, an electrical engineer at the University of Applied Sciences of Southern Switzerland in Manno, who studies visible-light communications.

Harald Haas, who researches mobile communications at the University of Edinburgh, UK, plans to test a visible-light system in hospitals within the next year. Patients will wear wristbands that monitor their temperature and relay the data using LEDs that communicate with the hospital's lighting.

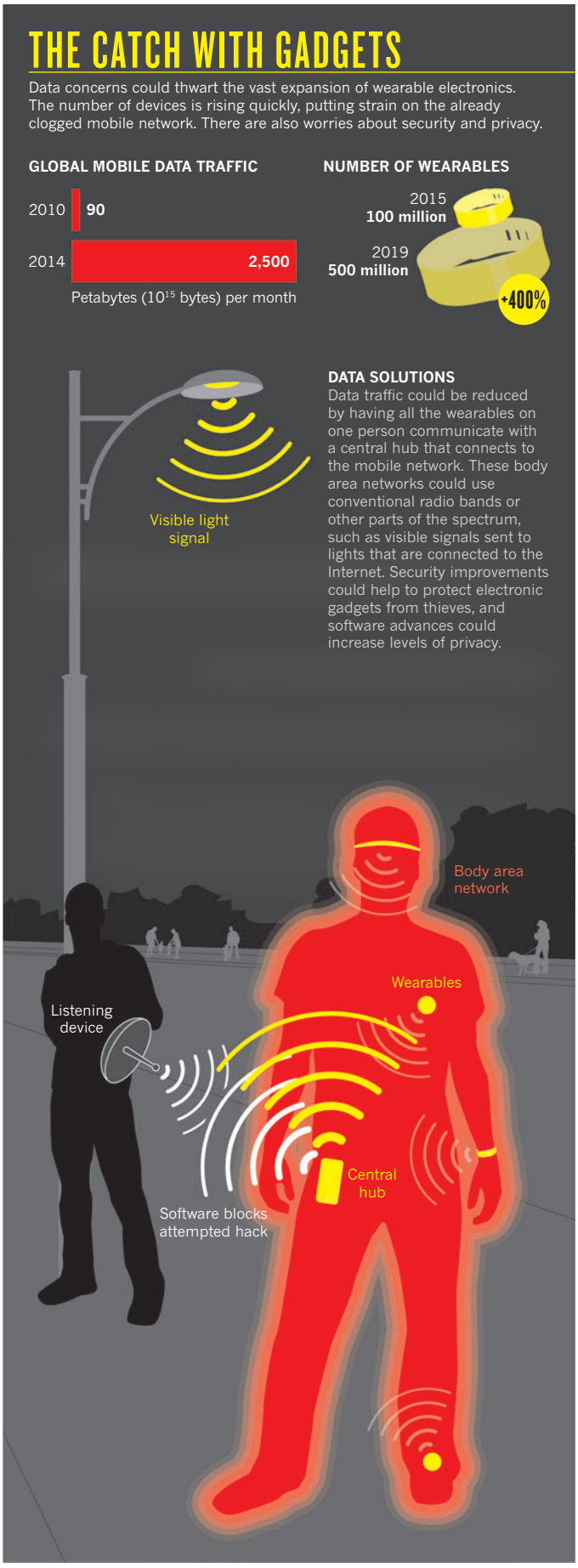
A broader approach might have wearable devices from many people relaying information to each other rather than having each connect to the Internet. This concept underpins the multitiered networks promised by the much-vaunted fifth-generation (5G) mobile-communication systems that are predicted to be up and running in many parts of the world by 2020. In situations where crowds of people are trying to access the same content — travel information after a sports match, for instance — one device could act as a 'seed', distributing the data to others in this network, which would reduce the number of times the data need to be downloaded from the Internet.

One of the most attractive approaches makes devices smarter about when and how they use communication channels. These 'cognitive radios' sniff out underused regions of bandwidth and opportunistically hop into those gaps, speeding up communications. To reach their optimum potential, bandwidths would need to be more open, so that devices could jump onto a licensed frequency to communicate, and then drop off the spectrum when someone with higher priority enters. Although techniques based on this principle have been used for decades, cognitive radio will take it to a new level of efficiency, with devices smart enough to negotiate with each other to divvy up the available spectrum.

Cognitive radios have great potential, but their development in the wearables realm is being held back by a lack of accepted standards and protocols for how this frequency hopping might work in practice, says Ekram Hossain, an electrical engineer at the University of Manitoba, Canada. "Until there is a standard, there won't be products," says Hossain, who adds that the research needed to establish these standards is under way.

KEEPING SAFE

When 176,000 people swarmed through the Consumer Electronics Show in Las Vegas in January, some of the hottest items were the crop of new wearable devices, ranging from watches and glasses to the Pacifi-i, a smart pacifier, or baby soother, that monitors an infant's temperature



and transmits the data to a parent's phone. And if those parents were stressed out, they could try the Melomind headset, which is advertised to measure the brain's electrical activity, beam it to a phone and then select the most appropriate music to help the wearer relax.

Despite all the hype about wearables, there is also considerable scepticism about the gadgets available today. "Lots of people view wearables as just toys", says Puccinelli.

But signs point to them being much more useful in the near future, particularly in the medical arena. Wearables are increasingly measuring aspects of human physiology, providing electrical stimulation to the brain and even injecting medication. These applications come with potential risks for users.

A key hurdle for the wearable revolution arises from the wealth of personal data they gather about their users. Surveys show that users worry about how these devices invade their privacy, as they upload intimate data to potentially vulnerable servers owned by companies that could change their terms of service, be bought out or go out of business.

When the Pew Research Center, an independent fact-gathering organization in Washington DC, canvassed 1,600 experts in 2014 about the future of the Internet, many expressed similar worries. "The realities of this data-drenched world raise substantial concerns about privacy and people's abilities to control their own lives," according to the report. Those concerns have been compounded by some high-profile incidents, such as when users of Fitbit activity trackers allowed their activity logs to be publicly accessible, unwittingly revealing when they had sex. When that was realized in 2011, Fitbit quickly took action to fix the problem.

In another high-profile incident, the introduction of Google Glass headsets two years ago triggered concerns that users would capture images of passers-by without their knowledge. Researchers at the Center for Cybersecurity took this opportunity to apply their work on computer codes that enforce privacy policies. They built the wryly named FaceBlock app, which blocks out the faces of people who have requested privacy from photographs taken by Google Glass. But for this to work, a Google Glass owner would have to opt in by installing the app. So the only way for such a system to reliably provide privacy would be for manufacturers to make it standard and implement it with dedicated hardware, says Joshi. "Let's say that Google was to build in a feature like this into every Google Glass so that it would automatically obey these kinds of commands — then it would work."

Security concerns go hand in hand with privacy. Although encryption is becoming more pervasive and advanced, it is sometimes not used in low-cost wearable devices. Last year, researchers at the California-based information-management company Symantec, revealed that the location of many health monitors, including some from market leaders, can be easily tracked. And some of them wirelessly communicate passwords in clear text, which makes them vulnerable to hacking. Even if a health monitor is encrypted, the smartphone or hub device that links it to the Internet could also be a weak point, either because of unnecessarily broad permissions or because of malware.

"If you're not encrypting the data you're definitely not secure," says Bogdan Carbunar, a security researcher at Florida International University in Miami. "Even if you're encrypting the data you can still not be secure." Carbunar worked with a team, including a researcher from IBM, on security holes in two popular low-cost wearable fitness devices, the Fitbit Ultra and the Garmin Forerunner. They found that by impersonating the devices' trusted webservers, they could fool the gadgets into uploading false data — even nonsensical numbers such as millions of steps in one day (see M. Rahman *et al. IEEE Trans. Mobile Comput.* http://doi.org/636; 2015).

The researchers also found that they could inject data onto a tracker of their own, which would compromise data accuracy, something that could become a problem if fitness data are tied to health-insurance premiums, as they have been in some companies. Fitbit told *Nature* that it had been aware of the problem, which has been addressed in subsequent products. Garmin did not respond to requests for comment.

According to Carbunar, security adds costs for manufacturers in terms of money, development time, device size and power consumption. But researchers are pushing to minimize those costs. After working out how to hack the devices, Carbunar and his team devised a way to keep them safe. They developed SensCrypt, an encryption protocol designed specifically for low-energy fitness trackers that reduces communications costs. It uses a procedure called symmetric key encryption to protect against remote attacks and to provide some security even if the device is stolen and tampered with. The researchers were unable to implement it on Fitbit or Garmin devices because they use closed-source code, but have tested their system on an open-source proxy.

WITH EVERYTHING FROM TOASTERS TO CARS NOW CONNECTING WIRELESSLY TO THE INTERNET, DEMANDS ON A FINITE BANDWIDTH ARE RAPIDLY STRAINING THE SYSTEM.

Even with high levels of encryption, devices could still be vulnerable to attack, says Bart Preneel, a cryptographer at the KU Leuven and iMinds research centre in Belgium. Preneel specializes in understanding and preventing side-channel attacks: attempts by hackers to infiltrate mobile devices by detecting fluctuations in the power usage and using these to calculate encryption keys and other secure information. "These attacks can be made at a distance of 10 or 20 metres," he says. This type of attack was discovered around 20 years ago in relation to bank cards, but ways of preventing it are not implemented in many wearable devices, particularly implanted medical technology.

Some companies have tried to improve security on mobile devices and wearables by equipping them with biometric devices such as fingerprint readers and iris scanners. But even these are insecure: researchers and hackers have shown how high-resolution cameras can capture someone's iris from a distance and how to steal a fingerprint using a phone's camera.

But Preneel says that biometrics are promising for encryption if designers focus on measures that are not so easy to discover. There are already wearables that authenticate users on the basis of their heartbeat pattern. In the long run, Preneel envisages using internal signals from the body, such as DNA or the internal microbial community, to pair with wearable gadgets so that the devices would unlock only when in close proximity to the owner.

With these kinds of improved security — and many upgrades in communications networks — a lost tourist in the future would stand a better chance of getting their wearables to work in a crowded plaza. Tom would easily be able to summon a map of the city on his lenses and would know his personal data were safely encrypted. Following the highlighted route, he might even make it to the station with enough time to get a coffee and charge his gadgets. It may not be the technological utopia imagined by some wearables enthusiasts, but at least he will catch his maglev. ■

Kat Austen *is a freelance writer in Berlin.*