My Pacemaker Is Tracking Me From Inside My Body
Cloud-connected medical devices save lives, but also raise questions about privacy, security, and oversight. An Object Lesson.

By: Neta Alexander

A month before turning 34, I received an unexpected birthday gift: a cloud-connected pacemaker. It sits in a tiny pocket in the left side of my chest, just above my heart. Silently and diligently, the device emits electrical pulses to make sure my heart rate never again plummets below 25 beats per minute.

The idea of a battery-equipped, internet-connected device living forever inside my chest both terrifies and fascinates me. When people say, “I’ll die if I lose my iPhone,” they never mean it literally. But I really might die without this smart gadget. I’m also at risk in other ways. A wireless pacemaker can be hacked, or, as recently happened in Ohio, become legal evidence that incriminates its user.

There is a crucial difference between my device and more ubiquitous digital technologies: I never made the choice to implant the pacemaker in my body. I’m grateful to the hardworking doctors who minimized my pain and helped me get better. At the same time, the device they installed raises questions that now haunt me. It’s not clear who might have access to data about my pulse, my health, and possibly my whereabouts—data generated by a device inside me.

* * *

Arriving at the ICU with a dangerously slow pulse, I was alarmed to find out I was suffering from a life-threatening condition called complete heart block. Learning that treatment would require a permanent pacemaker was no less of a surprise. I have nothing in common with the 76-year-old poster boy of pacemaker research, the former vice president Dick Cheney. Like Cheney, who survived five heart attacks, most pacemaker users are elderly—not grad students in their early 30s.

This might explain why the manufacturer of my pacemaker, the large medical-device company Medtronic, boasts that the device can be monitored remotely by health-care providers or worried family members. This tracking capacity could assuage anxiety, but it also raises some concerns about privacy and longevity.

Since the pacemaker was approved for Medicare reimbursement in 1966, there has been a sharp rise in the number of medical conditions that might lead to its installation. In 1984,
treatment guidelines from the American College of Cardiology called pacemakers at least a “reasonable” tool for treating 56 heart conditions. By 2008, the list had expanded to 88. Between 1993 and 2009, nearly 3 million Americans had pacemakers implanted.

Despite the growing number of pacemakers, not to mention the recent introduction of wireless cardiovascular devices like mine, their long-term effects, risks, and proprietary design are rarely discussed with new patients or their family members. Lior Jankelson, a physician at New York University’s cardiac-electrophysiology center, told me that every new pacemaker implanted in the United States is cloud-connected. “As a result,” Jankelson explains, “there are at least tens of thousands of Americans with cloud-connected devices that could be monitored from afar.” First, let’s save your life, the medical establishment might surmise, and later we can chitchat about how having a wireless, subdermal implant for the rest of that life might expose you to hacking, infections, and other health hazards.

My tiny device constantly collects data, which is automatically sent to my bedside monitor whenever my doctors schedule a remote-monitoring appointment. During these appointments, which take place every four to six months, the monitor sends my metrics to a secure server. A doctor examines the transmitted data and notifies me by phone if any further action is needed. The patient manual explains it like this: “Sending heart-device information using wireless technology does not require you to interact with your monitor. The process is silent and invisible. Clinics typically schedule the automatic process to occur while you sleep.”

That language is meant to reassure me that living with a wireless pacemaker is an effortless endeavor. But to me, the idea that my hidden chest box “talks” to others in my sleep is the stuff of nightmares. What is the device sending to the cloud, and what is the cloud sending back to it? It is impossible to know for sure whether my data is protected. As the security researcher Marie Moe recently wrote in Wired, “Part of the problem with doing security research in this field is that the medical devices appear as black boxes. How can I trust the machine inside my body when it is running on proprietary code and there is no transparency?”

Moe mentions that in 2008, a group of researchers at the University of Michigan proved that it is possible to extract sensitive personal information from a pacemaker—or even to threaten the patient’s life by changing the pacing behavior or turning it off. Other medical devices are also vulnerable. In 2011, Jay Radcliffe, an independent security researcher, revealed a security vulnerability in a Medtronic insulin pump that could allow an attacker to take control of it.

Aware of these alarming scenarios, in 2013 Cheney told CBS’s 60 Minutes that his doctors disabled his wireless pacemaker to thwart hacking and to protect him from possible assassination attempts. Riffing on a fictional assassination by pacemaker depicted on the TV show Homeland, Cheney stated that he found the plotline to be “an accurate portrayal of what was possible.”
Health providers can review my data from afar, and unauthorized hackers might have access to it, too. But it proved surprisingly difficult to access these medical records myself. After calling both Medtronic and the hospital in which my pacemaker was implanted, I was told I would have to sign a release form and wait for its approval before the data could be sent to me (via postal mail, no less). The process might take several weeks, and I would have no way of knowing whether the delivered data would be partial or complete. Just as Google or Facebook retains more data than it reveals, so even gadgets inside one’s body are gradually shifting control of personal information from users to corporations.

Any downsides to this trend are repeatedly denied by the medical-device manufacturers and cardiologists I spoke with. When I asked a Medtronic representative if I had to take the monitor with me for a two-week trip to the Middle East, he tried to convince me to “sign up to our new mobile app, which lets you download the data via a small, handheld monitor.” It’s a relief that I can travel safely around the world, but the long-term risks of connected monitoring systems are not part of the doctor-patient conversation. My phone conversation with Medtronic reminded me of routine conversations with my internet or cable providers, when overworked and underpaid representatives desperately tried to sell me “our brand-new package” for a “once-in-a-lifetime deal.”

The potential threats posed by hackers are distressing, but so is the notion that my pulse has been monetized. Medtronic is a public company with 84,000 employees in about 160 countries, serving more than 50,000 patents. The company, which moved its headquarters from Minnesota to low-tax Ireland in 2015, defines making “a fair profit” as one of the goals in its official mission statement. With revenues totaling $10.5 billion from cardiac and vascular devices in 2017 alone, it seems to be succeeding.

Data monitoring is threatening because those subject to it don’t know what information is being collected, for what reason, and by whom. And unlike iPhone or Amazon Echo users, I cannot just choose to stop using my connected pacemaker. In a way, my heart is no longer entirely mine: I share it with both Medtronic and with the U.S. hospital in which it was implanted. As an immigrant in America at a time when foreign status is uncertain, I can’t help but wonder if my pulse might one day betray me. Might it show I visited a place I was not supposed to, or dared meet someone from a hostile country?

In the meantime, patients are left without answers. I woke up to a life that depends on a fancy metronome and the invisible infrastructure sustaining it: replaceable batteries, bedside monitors, secure servers, Wi-Fi connectivity. There are millions more people who depend on wireless medical implants, our bodies talking constantly to medical companies and data brokers. If our bodies can talk to them, it shouldn’t be outlandish to imagine they might return the favor.