RISK OF EXPOSURE

When new or dangerous infectious diseases strike, public health often trumps personal privacy

By **Martin Enserink**

Few things can make you famous—or notorious—as fast as an encounter with the Ebola virus. New York physician Craig Spencer saw his daily life dissected by the media, which noted an evening at a Brooklyn bowling alley, a meal at the Meatball Shop, and rides on the 1, A, and L subway trains. Kaci Hickox, a nurse from Maine, was publicly attacked for defying a quarantine that scientists agreed made little sense. *The Daily Mail*, a British tabloid, delved into the past of freelance cameraman and Ebola patient Ashoka Mukpo and dug up salacious details about his parents' love life.

Protecting medical information is tricky enough, but when you fall ill during an outbreak of a new or particularly scary disease, everything appears to become fair game. It's not just reporters who pore over your life. Doctors and public health officials, too, want to know where you have been, what you have done, and with whom. The more widely they share any of that information, the greater the risk to your privacy.

A rise in the number of new and re-emerging diseases in the past 2 decades—including SARS, MERS, and several influenza subtypes—has brought such problems painfully into focus, and the advent of social media and cell phone cameras has increased the pressure. When ambulance workers clad in white protective suits picked up a man at his home in the Dutch city of Maastricht on 26 October 2014, for instance, "it was on Twitter in 20 minutes," says George Haringhuizen, a lawyer at the National Institute for Public Health and the Environment in Bilthoven, the Netherlands. Regional health officials were quick to deny claims that Ebola was involved.

Reining in bloggers and Twitter users may not be easy. But even professional efforts to track outbreaks pose new threats to privacy. Information about specific patients—although anonymized—is now shared worldwide on public e-mail lists for emerging diseases such as ProMED, which often recirculates newspaper stories from around the world. Although it always redacts patient names, says ProMED Editor Larry Madoff, a simple Google search is enough to find the original story with those names.

There is a growing need for global ethical standards for governmental disease surveillance, akin to what the Declaration of Helsinki provides for medical research, says Amy Fairchild, a historian at Columbia University who studies public health policy. Fairchild co-chairs a group of ethicists and public health experts assembled by the World Health Organization (WHO) to make recommendations on the subject; privacy will be a key issue, she says.

UNTIL THE 1960S, major U.S. newspapers routinely printed the names and addresses of people with infectious diseases such as polio, Fairchild says. It wasn't until the 1970s, when governments and other organizations began storing large amounts of electronic data on citizens, including medical records, that privacy emerged as a political issue. Heart-wrenching cases of stigmatization and discrimination against AIDS patients in the 1980s—which led many to hide their HIV status—galvanized support for the protection of medical privacy.

Many countries now have complex laws and regulations governing how and when medical information can be shared, such as the Privacy Rule of the U.S. Health Insurance Portability and Accountability Act, passed in 1996. Yet there still is a "huge tension" between the worlds of clinical care—where doctors try to protect individual patients—and public health, which tries to protect communities, says bioethicist Arthur Caplan of New York University's Langone Medical Center in New York City—especially during disease outbreaks. "Privacy doesn't fit well in the mindset of people in public health," he says. "For them, the question is: How much can I get away with without privacy going completely out of the window?"

Disease detectives at the U.S. Centers for Disease Control and Prevention, for instance, can't track down a mysterious outbreak without having as much information about the patients as possible. At the same time, governments can't know if public health policies work without gathering detailed data about disease incidence.

But because of privacy concerns, doctors sometimes don't comply with requirements to notify health authorities when they diagnose a patient with a reportable disease, of which there are about a hundred in the United States. A qualitative study conducted in Canada at the height of the 2009 influenza pandemic showed that some doctors were surprisingly reluctant to report patients with flulike symptoms, as they were supposed to. "I think the bottom line for most family physicians is we will not share names, addresses, or phone numbers, period, without individual patient consent," one said in a focus group.

There are debates about how reported data can be used as well. New York state, for example, requires doctors not only to report HIV diagnoses, but also to forward lab results such as viral loads and CD4 cell counts. When such reports stop coming in for a given patient, researchers say, it's a sign they may have dropped out of treatment, which could help the virus rebound and put sex partners at risk. A 2013 study showed that of 409 dropouts, 57% were brought back into care after they had been traced and contacted—but some believe that's crossing a line.

EVEN WHEN DOCTORS or government agencies treat health data discreetly, patient identities often become known—in their neighborhoods, towns, or in the press. When federal agents go around the block to trace the contacts of an Ebola patient, it's usually not hard to find out who the patient is. Europe's very first AIDS patient, who died in 1976, was long known as "the Norwegian sailor," and later by an anagram of his real name, used in Edward Hooper's book *The River*—until journalists revealed his name around a decade ago. (The man is believed to have picked up HIV in West Africa in the early 1960s; his wife and one

THE PRIVACY ARMS RACE

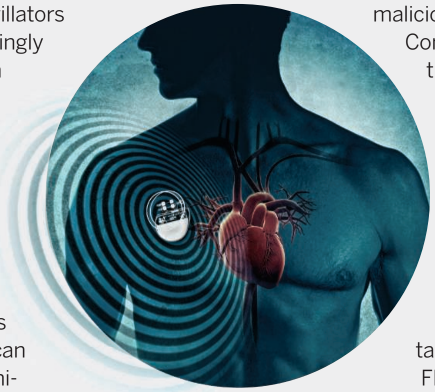
Could your pacemaker be hackable?

By **Daniel Clery**

In a 2012 episode of the TV series *Homeland*, Vice President William Walden is assassinated by a terrorist who hacks into his Internet-enabled heart pacemaker and accelerates his heartbeat until he has a heart attack. A flight of fancy? Not everyone thinks so.

Internet security experts have been warning for years that such devices are open to both data theft and remote control by a hacker. In 2007, Vice President Dick Cheney's cardiologist disabled the wireless functionality of his pacemaker because of just that risk. "It seemed to me to be a bad idea for the vice president to have a device that maybe somebody on a rope line or in the next hotel room or downstairs might be able to get into—hack into," said the cardiologist, Jonathan Reiner of George Washington University Hospital in Washington, D.C., in a TV interview last year.

Medical devices such as insulin pumps, continuous glucose monitors, and pacemakers or defibrillators have become increasingly small and wearable in recent years. They often connect with a hand-held controller over short distances using Bluetooth. Often, either the controller or the device itself is connected to the Internet by means of Wi-Fi so that data can be sent directly to clinicians. But security experts have demonstrated that with easily available hardware, a user manual, and the device's PIN number, they can take control of a device or monitor the data it sends.



Medical devices don't get regular security updates, like smart phones and computers, because changes to their software could require recertification by regulators like the U.S. Food and Drug Administration (FDA). And FDA has focused on reliability, user safety, and ease of use—not on protecting against malicious attacks. In a Safety Communication in 2013, the agency said that it "is not aware of any patient injuries or deaths associated with these incidents nor do we have any indication that any specific devices or systems in clinical use have been purposely targeted at this time." FDA does say that it "expects medical device manufacturers to take appropriate steps" to protect devices. Manufacturers are starting to wake up to the issue and are employing security experts to tighten up their systems. But unless such steps become compulsory, it may take a fatal attack on a prominent person for the security gap to be closed. ■

IMAGES: (OPPOSITE AND RIGHT) WILLIAM DUKE (2)

of his two daughters succumbed to AIDS as well.) The case still upsets Stig Frøland, a researcher at the Rikshospitalet in Oslo who published about the family and says he tried hard to protect their identity. Still, Frøland isn't surprised, "in view of my experience with the very aggressive attitude from national and international media through the years."

Craig Spencer's identity was revealed by the press, too. (A Twitter search suggests the *New York Post* identified Spencer first, 8 hours after his hospitalization, simply citing "sources," followed shortly after by the New York *Daily News*.) The details that the health department subsequently made public about Spencer's movements before he fell ill were a clear invasion of his privacy, Fairchild says—and an unwarranted one, because he didn't have symptoms at the time and wasn't infectious. (Spencer, who asked the media to respect his right to privacy after he recovered, did not respond to requests for comment.)

Mukpo, by contrast, agreed that his name could be released after he got Ebola, in part hoping it might help get him repatriated from Liberia, where he became infected. "Honestly, though," he adds, "me remaining anonymous would never have been a realistic option," given that he worked for NBC and knew many journalists.

The upcoming WHO report, expected in 2016, will come up with recommendations for disease surveillance in general, not just for infectious diseases. But the panel may well borrow some pages from a similar WHO report, published in 2013, on the ethics of HIV surveillance, which remains an extremely sensitive issue today. That document recommended that the names of HIV patients be reported only for public health purposes—not for discrimination or criminalization—and only when confidentiality of the data is assured. It also said that people's right not to participate in surveillance should be respected as much as possible.

The tension between privacy and public health will always remain, Caplan says, but preventing stigmatization and other negative consequences could help relieve some of the worries. "If you're not going to lose your job, lose your house, lose your mate, there's less reason to worry about your privacy," he says. And eventually, he says, people may care less than they do today about whether officials track their movements and contacts. Young people already share massive amounts of information online—including where they are, what they're doing, and who they're with. ("When I ask them if they aren't worried about their privacy, I get a condescending look," Caplan says.) Medical privacy, too, will become a "quaint notion," Caplan predicts.

For Mukpo—who noted the irony when *Science* e-mailed him to ask questions about his privacy—the exposure was actually a mixed experience. Although it was "very disconcerting to become such a public figure so quickly," he did use the media spotlight to raise awareness about the Ebola situation in Africa. What's more, "the publicity also was an opportunity to see just how many amazing people I have in my life," he adds. "The outpouring of concern was humbling." ■

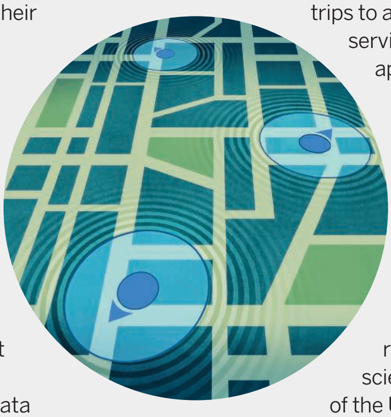
THE PRIVACY ARMS RACE

Hiding in plain sight

By **Jia You**

Whether they're looking for nearby restaurants, wondering what to wear, or finding the fastest route, most people allow their smart phones to send their GPS locations to Yelp, AccuWeather, or Google Maps without a second thought. But these data can be shared with advertisers and other third parties that profile users' movement patterns, often without their knowledge.

Even anonymizing people's location data doesn't necessarily protect their privacy. When New York City released anonymized data on more than 173 million taxi trips in response to a Freedom of Information Act request in March, researchers quickly combined the data with known reference points—addresses, for example—to pinpoint celebrities' cab trips and identify who frequented local strip clubs.



Computer scientists are devising countermeasures. CacheCloak, a system developed by researchers at Duke University in Durham, North Carolina, throws off tracking efforts by hiding users' actual location data. When you want to find, say, nearby restaurants, CacheCloak doesn't send Yelp or Google your exact GPS coordinates, but an entire path that it predicts you will take. That path is made to intersect with predicted paths from other users, so that the service sees requests from a series of interweaving paths where a driver can go either way at each crossing, and cannot track any single user. But consumers can still receive relatively accurate results.

A slightly different camouflage strategy is to send dummy locations along with a user's real location. Researchers at Microsoft, for instance, have built an algorithm that can generate realistic car trips in Seattle based on real GPS data on 16,000 drives taken by about 250 volunteer drivers in the area. The dummy trips have plausible start and end points—no stopping in the middle of a highway—adhere to speed limits, and deliberately follow slightly non-optimal routes, so that a filter can't easily pick out the false trips from the real ones. A mobile phone would draw on the library of routes to send both the user's actual location and points from many dummy trips to a cloud-based location service like Google Maps. The app responds—say, to a request for traffic warnings—for all locations, but users can use the answers they need and disregard the rest.

The downside of the strategy is that such dummy searches can result in embarrassment, says computer scientist Michael Herrmann of the University of Leuven in Belgium. For example, many people might not want their trip to the library masked as a visit to an HIV testing site.

In a third strategy, algorithms can simply send imprecise location data to services, cloaking a user's whereabouts in 1-kilometer squares rather than revealing precise GPS coordinates. But that has the obvious drawback of decreasing the quality of an online service, Herrmann says. For a weather app, your exact location may not matter, but if you're on foot and need to find a nearby ATM, precision is crucial.

In the end, human movements are often so predictable that they are hard to conceal. Location-hiding techniques are most valuable when you want to hide one-off trips, Herrmann says. But when it comes to protecting the location of your home and workplace, you might as well give up on privacy. ■

IMAGE: WILLIAM DUKE