The New York Times | https://nyti.ms/2KNWrZd

Banks and Retailers Are Tracking How You Type, Swipe and Tap

By Stacy Cowley

Aug. 13, 2018

When you're browsing a website and the mouse cursor disappears, it might be a computer glitch — or it might be a deliberate test to find out who you are.

The way you press, scroll and type on a phone screen or keyboard can be as unique as your fingerprints or facial features. To fight fraud, a growing number of banks and merchants are tracking visitors' physical movements as they use websites and apps.

Some use the technology only to weed out automated attacks and suspicious transactions, but others are going significantly further, amassing tens of millions of profiles that can identify customers by how they touch, hold and tap their devices.

The data collection is invisible to those being watched. Using sensors in your phone or code on websites, companies can gather thousands of data points, known as "behavioral biometrics," to help prove whether a digital user is actually the person she claims to be.

To security officials, the technology is a powerful safeguard. Major data breaches are a near-daily occurrence. Cyberthieves have obtained billions of passwords and other sensitive personal information, which can be used to steal from customers' bank and shopping accounts and fraudulently open new ones.

"Identity is the ultimate digital currency, and it's being weaponized at an industrial scale," said Alisdair Faulkner, one of the founders of ThreatMetrix, which makes fraud detection software for large merchants and financial companies. Many of his company's customers are now using or testing behavioral biometric tools, he said.

The angle at which you hold your device is one of the many biometric markers that can be measured. Andrew Roberts

Privacy advocates view the biometric tools as potentially troubling, partly because few companies disclose to users when and how their taps and swipes are being tracked.

“What we have seen across the board with technology is that the more data that’s collected by companies, the more they will try to find uses for that data,” said Jennifer Lynch, a senior lawyer for the Electronic Frontier Foundation. “It’s a very small leap from using this to detect fraud to using this to learn very private information about you.”

The Royal Bank of Scotland, one of the few banks that will talk publicly about its collection of biometric behavioral data, started testing the technology two years ago on private banking accounts for wealthy customers. It is now expanding the system to all of its 18.7 million business and retail accounts, according to Kevin Hanley, the bank’s director of innovation.

When clients log in to their Royal Bank of Scotland accounts, software begins recording more than 2,000 different interactive gestures. On phones, it measures the angle at which people hold their devices, the fingers they use to swipe and tap, the pressure they apply and how quickly they scroll. On a computer, the software records the rhythm of their keystrokes and the way they wiggle their mouse.

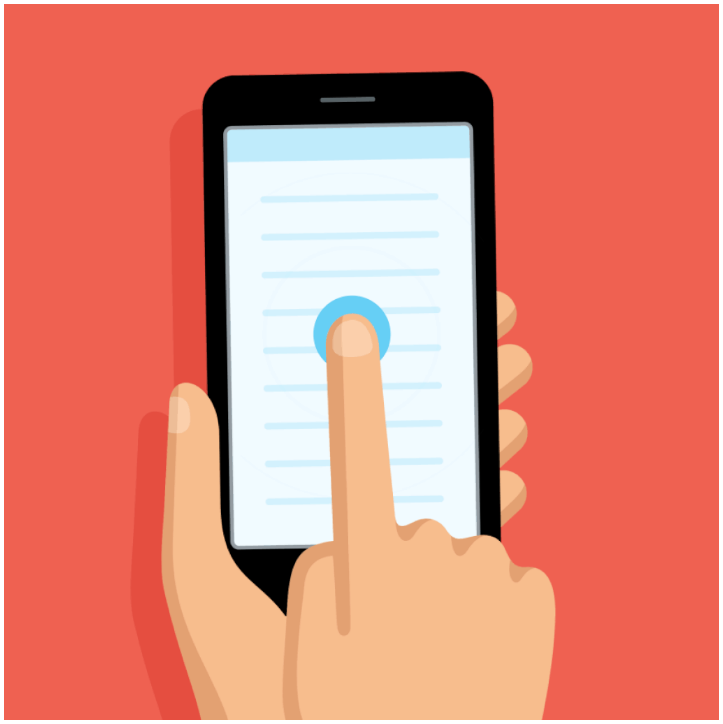
R.B.S. is using software designed by a small New York company called BioCatch. It builds a profile on each person's gestures, which is then compared against the customer's movements every time they return. The system can detect impostors with 99 percent accuracy, BioCatch says.

A few months ago, the software picked up unusual signals coming from one wealthy customer's account. After logging in, the visitor used the mouse's scroll wheel — something the customer had never done before. Then the visitor typed on the numerical strip at the top of a keyboard, not the side number pad the customer typically used.

Alarm bells went off. The R.B.S. system blocked any cash from leaving the customer's account. An investigation later found that the account had been hacked, Mr. Hanley said.

"Someone was trying to set up a new payee and transfer a seven-figure sum," he said. "We were able to intervene in real time and stop that from happening."

That case was unusually blatant. A user's behavior isn't constant; people act differently when they're tired, injured, drunk, distracted or in a hurry. The way people type at an office desk is distinct from when they're slumped on their sofa at home.



Biometric software can also determine the pressure you tend to apply to your phone when you tap and type. Andrew Roberts

Behavioral monitoring software churns through thousands of elements to calculate a probability-based guess about whether a person is who they claim. Two major advances have fed its growing use: the availability of cheap computing power and the sophisticated array of sensors now built into most smartphones.

The system's unobtrusiveness is part of its appeal, Mr. Hanley said. Traditional physical biometrics, like fingerprints or irises, require special scanning hardware for authentication. But behavioral traits can be captured in the background, without customers doing anything to sign up.

BioCatch occasionally tries to elicit a reaction. It can speed up the selection wheel you use to enter data like dates and times on your phone, or make your mouse cursor disappear for a fraction of a second.

“Everyone reacts a little differently to that,” said Frances Zelazny, BioCatch's chief strategy and marketing officer. “Some people move the mouse side to side; some people move it up and down. Some bang on the keyboard.”

Because your reaction is so individual, it's hard for a fraudulent user to fake. And because customers never know the monitoring technology is there, it doesn't impose the kind of visible, and irritating, roadblocks that typically accompany security tests. You don't need to press your thumb on your phone's fingerprint reader or type in an authentication code.

“We don't have to sit people down in a room and get them to type under perfect laboratory conditions,” said Neil Costigan, the chief executive of BehavioSec, a Palo Alto, Calif., company that makes software used by many Nordic banks. “You just watch them, silently, while they go about their normal account activities.”

Businesses call that a “frictionless” experience. Privacy watchdogs call it dangerous.

Biometric systems can sometimes detect medical conditions. If a customer with a once-steady hand develops a tremor, her automobile insurance company might get worried. That's potentially a problem if the customer's bank, which detected the tremor through its security software, is also her insurer.

“This is the kind of data that usually has some kind of consumer protections around it, but here there's none at all,” said Pam Dixon, the executive director of the World Privacy Forum. “Companies are using these systems with no notice of any kind.”

In most countries, there are no laws governing the collection and use of biometric behavioral data.

Even Europe's new privacy rules have exemptions for security and fraud prevention. A new digital privacy law in California includes behavioral biometrics on the list of tracking technologies companies must disclose if they collect, but it does not take effect until 2020.

Banks and merchants sometimes store their customers' biometric data internally. In many cases, though, they allow the outside vendors they work with to hold it. That magnifies the risks, Ms. Dixon said.

BioCatch has profiles on about 70 million individuals and monitors six billion transactions a month, according to Ms. Zelazny, the company's strategy executive. American Express, an investor in BioCatch, recently began using its technology on new account applications.

Some of BioCatch's rivals have even larger networks. Forter, a New York start-up that sells online fraud detection software incorporating behavioral biometrics to big retailers, said its database has records on 175 million people from more than 180 countries. Another competitor, NuData, was acquired last year by Mastercard.

On your computer, software can track your mouse habits, including the speed and rhythm of your cursor tracking. Andrew Roberts

More than a dozen technology vendors, from under-the-radar start-ups to giants like I.B.M., have built behavioral biometrics into the security software they sell to retailers and banks.

The technology can be useful for rooting out fraud even without personal data on individual customers.

On new account applications, for example, behavioral biometric systems pay close attention to where and when applicants pause. A legitimate applicant typically types personal information — their name, their address, their Social Security number — fluidly, with few breaks. A scammer will often either cut and paste or take breaks to consult their notes.

“This used to be like science fiction,” said Ryan Wilk, a NuData employee who is now a Mastercard vice president. “When we described what we did, people would give us looks like, ‘Is this real?’ Now, it’s become not just a gimmick but a major technology in the financial industry. Lots of big companies are using it.”

A version of this article appears in print on , Section B, Page 1 of the New York edition with the headline: Type Carefully. Your Bank Is Watching.