COMMONLIT

Name: _____ Class: _____

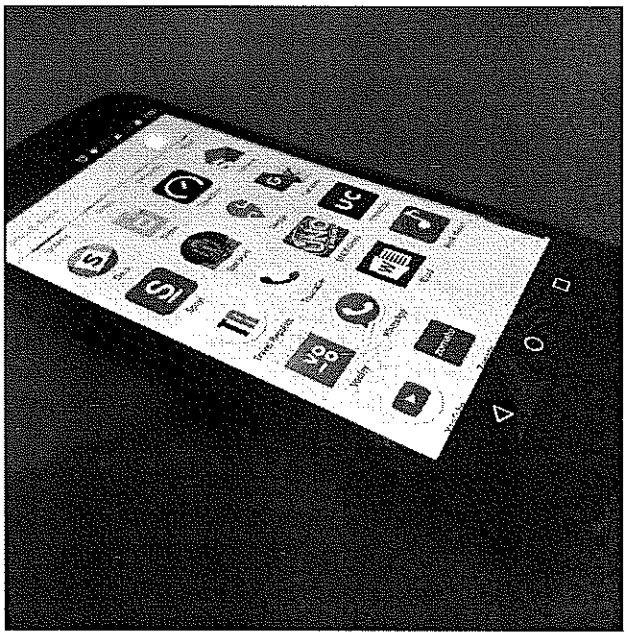
# Smartphones Put Your Privacy At Risk

*Devices can divulge a whole lot of data on your comings and goings*

By Maria Temming
2018

*In this informational text, Maria Temming discusses how smartphones collect information about people and the different ways that information is being used. As you read, take notes on the different ways that smartphones collect information about users.*

[1] Consider everything your smartphone has done for you today. Counted your steps? Transcribed notes? Navigated you somewhere new?



*"Untitled" by Matam Jaswanth is licensed under CC0.*

Smartphones make for versatile[1] pocket assistants. That's because they're equipped with a suite of sensors.[2] And some of those sensors you may never think — or even know — about. They sense light, humidity, pressure, temperature and other factors.

Smartphones have become essential companions. So those sensors probably stayed close by throughout your day. They sat in your backpack or on the dinner table or nightstand. If you're like most smartphone users, the device was probably on the whole time, even when its screen was blank.

"Sensors are finding their ways into every corner of our lives," says Maryam Mehrnezhad. She's a computer scientist at Newcastle University in England. That's a good thing when phones are using their powers to do our bidding. But the many types of personal information that phones have access to also makes them potentially powerful spies.

[5] Online app store Google Play has already discovered apps that are abusing their access to those sensors. Google recently booted 20 apps from Android phones and its app store. Those apps could record with the microphone, monitor a phone's location, take photos and then extract the data. And they could do all of this without a user's knowledge!

Stolen photos and sound bites pose obvious privacy invasions. But even seemingly innocent sensor data might broadcast sensitive information. A smartphone's motions might reveal what a user is typing. Or it might disclose someone's location. Even *barometer* readings could be misused. These readings subtly shift with increased altitude. That could give away which floor of a building you're on, suggests Ahmed Al-Haiqi. He's a security researcher at the National Energy University in Kajang, Malaysia.

1. **Versatile** *(adjective)* having many uses or applications
2. a set of devices that collect physical and chemical information with uniform design that can share information

## Message revealed

Motion detectors are some of the tools within smartphones that are collecting data. These include their accelerometer[3] (Ak-sell-ur-AHM-eh-tur) and the rotation-sensing gyroscope.[4] Such bits of technology could be prime tools for sharing data without your knowing it.

One reason: They're not permission-protected. That means a phone's user doesn't have to give a newly installed app permission to access those sensors. So motion detectors are fair game for any app downloaded onto a device.

In an April 2017 study, Mehrnezhad's team at Newcastle showed that touching different regions of a screen makes the phone tilt and shift just a tiny bit. You may not notice it. But your phone's motion sensors will. The data they collect may "look like nonsense" to the human eye, says Al-Haiqi. Yet clever computer programs can tease out patterns in that mess. They can then match segments of motion data to taps on various regions of the screen.

[10] For the most part, these computer programs are algorithms[5] that make up a type of *machine learning*,[6] Al-Haiqi says. Researchers first train the programs to recognize keystrokes. They do this by feeding the programs lots of motion-sensor data. Those data are then labeled with the key tap that produced a particular movement.

A pair of researchers built TouchLogger. It's an app that collects sensor data on a phone's orientation in space. It uses these data to figure out how a user had been tapping on a smartphone's number keyboard. In a 2011 test on phones made by a company in Taiwan, called HTC, TouchLogger figured out more than 70 percent of key taps correctly.

Since then, more studies have come out showing similar results. Scientists have written code to infer keystrokes on number and letter keyboards for different types of phones. In one 2016 study, Al-Haiqi's team reviewed how successful these efforts were. And they concluded that only a snoop's imagination limits the ways motion data could be translated into key taps. Those keystrokes could reveal everything from the password entered on a banking app to the contents of a text message.

A more recent application used a whole fleet of smartphone sensors to guess PINs. (A PIN is a sequence of numbers used to access a bank account.) The app analyzed a phone's movement. It also noted how, during typing, the user's finger blocked the light sensor. When tested on a pool of 50 PIN numbers, the app could discern keystrokes with 99.5 percent accuracy. The researchers reported this in December 2017 on the Cryptology ePrint Archive.

Other researchers have paired motion data with microphone recordings. A phone's mic can pick up the soft sound of a fingertip tapping on a screen. One group designed a malicious[7] app. It could masquerade[8] as a simple note-taking tool. When the user tapped on the app's keyboard, the app covertly recorded the keys' input. It also recorded the simultaneous microphone and gyroscope readings. That let it learn the sound and feel to correctly diagnose each keystroke.

3. something that measures acceleration
4. a device that can measure the 3-dimensional position of something
5. a group of rules for solving a problem in a series of steps
6. a way in which computers learn from examples or experience
7. **Malicious** ***(adjective)*** intending to do harm
8. **Masquerade** ***(verb)*** to pretend to be something different

[15] The app could even listen in the background when the user entered sensitive info on other apps. This phone app was tested on Samsung and HTC phones. It inferred the keystrokes of 100 four-digit PINs with 94 percent accuracy.

Such high success rates come mostly from tests made in controlled settings, notes Al-Haiqi. Those tests assume that users will hold their phones a certain way each time or will sit down while typing. How these info-extracting programs fare in a wider range of real-world conditions remains to be seen. But the answer to whether motion and other sensors would open the door for new privacy invasions is "an obvious yes," he says.

## Tagalong

Motion sensors also can help map someone's travels, such as on a subway or bus ride. A trip produces motion data that are different from the more brief, jerkier movements of something like a phone being pulled from a pocket.

For a 2017 study, researchers designed an app to extract the data signatures of various subway routes. They used accelerometer readings from Samsung smartphones of people riding the subway in Nanjing, China.

A tracking app picked out which segments of the subway system a user was riding. It did this with an accuracy of 59 to 88 percent. How well it performed depended on how many subway stations the people rode through. (The app improved as the rides lengthened from three stations to seven stations long.) Someone who can trace a user's subway movements might figure out where the traveler lives and works. They might tell where the user shops or map out someone's entire daily schedule. It might even — if the app is tracking multiple people — figure out who the user meets at various places.

[20] Accelerometer data also can plot driving routes. And other sensors can be used to track people in more confined spaces.

One team, for instance, synced a smartphone mic and portable speaker. That let them create an on-the-fly sonar[9] system to map movements throughout a house. The team reported the work in a September 2017 study.

Selcuk Uluagac is an electrical and computer engineer. He works at Florida International University in Miami. "Fortunately, there is not anything like [these sensor spying techniques] in real life that we've seen yet," he notes. "But this doesn't mean there isn't a clear danger out there that we should be protecting ourselves against."

That's because the types of algorithms that researchers have used to comb through sensor data are getting more advanced and user-friendly all the time, says Mehrnezhad at Newcastle University. It's not just people with PhDs who can design these types of privacy invasions, she says. App developers who don't understand machine-learning algorithms can easily get this kind of code online to build sensor-sniffing programs.

What's more, smartphone sensors don't just provide snooping opportunities for cybercrooks who peddle[10] info-stealing software. Legitimate apps often harvest info to compile such things as your search-engine and app-download history. The makers of these apps sell that info to advertising companies and outside parties. They could use the data to learn aspects of a user's life that this person might want to keep private.

9. a system that detects an object by emitting sound pulses and measuring how long it takes for the echoes to return
10. sell

[25] Take a health-insurance company. It may charge more to insure someone who doesn't get much exercise. So "you may not like them to know if you are a lazy person or you are an active person," Mehrnezhad says. Yet with your phone's motion sensors, "which are reporting the amount of activity you're doing every day, they could easily identify what type of user you are."

## Sensor safeguards

It's getting ever easier for an untrustworthy party to figure out private details of your life from data they get from your phone's sensors. So researchers are devising ways to give people more control over what information apps can siphon[11] data from their devices.

Some safeguard apps could appear as standalone programs. Others are tools that would be built into future updates of the operating system for your phone's onboard computer.

Uluagac and his colleagues recently proposed a system called 6thSense. It monitors a phone's sensor activity. Then it alerts an owner when it detects unusual behaviors. Users train this system to recognize their phone's normal sensor behavior. This might include tasks like calling, Web browsing or driving. Then, 6thSense continually checks the phone's sensor activity against these learned behaviors.

That program is on the lookout for something odd. This might be the motion sensors reaping[12] data when a user is just sitting and texting. Then, 6thSense alerts the user. Users can check if a recently downloaded app is responsible for a suspicious activity. If so, they can delete the app from their phones.

[30] Uluagac's team recently tested a prototype[13] of 6thSense on Samsung smartphones. The owners of 50 of these phones trained with 6thSense to identify their typical sensor activity. The researchers then fed the 6thSense system examples of benign data from daily activities mixed with bits of malicious sensor operations. 6thSense correctly picked out the problematic bits more than 96 percent of the time.

Supriyo Chakraborty is a privacy and security researcher at IBM in Yorktown Heights, N.Y. His team devised DEEProtect for people who want more active control over their data. It's a system that blunts[14] the ability of apps to draw conclusions about user activity from a phone's sensor data. People could use DEEProtect to specify what their apps would be allowed to do with sensor data. For example, someone may want an app to transcribe speech but not identify the speaker.

DEEProtect intercepts whatever raw sensor data an app tries to access. It then strips those data down to only the features needed to make user-approved inferences.

Consider speech-to-text translation. For this, the phone typically needs sound frequencies and the probabilities of particular words following each other in a sentence. But sound frequencies could also help a spying app deduce a speaker's identity. So DEEProtect distorts the dataset before releasing it to the app. However, it leaves alone data on word orders. Those data have little or no bearing on a speaker's identity.

Users get to control how much DEEProtect changes the data. More distortion offers more privacy — but at a price: It degrades app functions.

11. to take and use something for your own purposes
12. **Reap** ***(verb)*** to gather something
13. a preliminary model
14. **Blunt** ***(verb)*** to make less sharp or accurate

[35] Giuseppe Petracca is a computer scientist and engineer at Pennsylvania State University in University Park. He and his colleagues took a different approach. They are trying to protect users from accidentally allowing sensor access to deceitful apps. Their security system is called AWare.

When they are first installed, apps have to get a user permission to access certain sensors. This might include the mic and camera. But people can be careless about granting those permissions, Uluagac says. All too often, "people blindly give permission," he says, to use the phone's camera or microphone. They may give no thought to why the apps might — or might not — need them.

AWare would instead request permission from a user before an app can access a certain sensor the first time a user provided a certain input. For instance, this might happen when you press a camera's button the first time after downloading an app. On top of that, the AWare system memorizes the state of the phone when the user grants that first permission. It remembers the exact appearance of the screen, the sensors that were requested and other information. That way, AWare can tell users if and when the app later attempts to trick them into granting unintended permissions.

The Penn State researchers imagined a crafty data-stealing app. It would ask for camera access when the user first pushes a camera button. But it would then also try to access the mic when the user later pushes that same button. The AWare system would realize the mic access wasn't part of the initial deal. It would then ask the user again if he or she would like to grant this additional permission.

Petracca and his colleagues tested AWare with people using Nexus smartphones. Those using phone equipped with AWare avoided unwanted authorizations about 93 percent of the time. That's compared with just 9 percent among people using smartphones with typical first-use or install-time permission policies.

## The Price of Privacy

[40] The security team in Google's Android division is also trying to mitigate[15] the privacy risks posed by app sensor data collection. Rene Mayrhofer is an Android security engineer in Austria at Johannes Kepler University in Linz. He and his colleagues are keeping tabs on the latest security studies coming out of university labs.

But just because someone has a successful prototype of a new smartphone-security system doesn't mean it will show up in future phone updates. Android hasn't incorporated any of these proposed sensor safeguards yet. That's because its security team is still looking for the right balance. The team wants to restrict access for nefarious[16] apps but not slow or degrade the functions of trustworthy programs, Mayrhofer explains.

"The whole [app] ecosystem is so big," he notes. "And there are so many different apps out there that have a totally legitimate purpose." Any kind of new security system that curbs an app's access to the phone's sensors, he says, could pose "a real risk of breaking" legitimate apps.

Tech companies may also be reluctant to adopt more security measures. Why? These extra protections can come at the cost of user friendliness. (AWare's additional permissions pop-ups, for instance.)

Mani Srivastava is an engineer at the University of California, Los Angeles. There's always a trade-off between security and convenience, he says. "You're never going to have this magical sensor shield [that] gives you this perfect balance of privacy and utility."

15. **Mitigate** *(verb)* to make less severe or serious
16. **Nefarious** *(adjective)* wicked or criminal

[45] But phones are relying on ever more — and more powerful — sensors. And algorithms for analyzing their data are becoming more wise. Because of this, even smartphone makers may eventually admit that the current sensor protections aren't cutting it. "It's like cat and mouse," Al-Haiqi says. "Attacks will improve. Solutions will improve." Then more clever attacks will emerge. And security teams will engineer still more clever solutions. And on and on it goes.

The game will continue, Chakraborty agrees. "I don't think we'll get to a place where we can declare a winner and go home."