Written by **C. Mitchell Shaw** on April 5, 2018

Internet Interlopers: It Isn't Just Facebook

While Facebook has been in the headlines over the past few weeks as a result of its practice of harvesting and misusing users' data, it is far from the only tech company guilty of "surveillance as a feature." Google, Microsoft, and others routinely vacuum up large amounts of personal data about those who use their services.

In the wake of revelations that at least 50 million (and possibly as many as 87 million) Facebook users had their personal data breached and used to manipulate the 2016 presidential election, the social-media giant began taking a beating. Users — both individuals and companies — began abandoning the platform. Stocks plummeted, costing the company 24 percent of its value and totaling $100 billion in losses. Though the market seems already to be forgiving the company, with stock prices rebounding slightly in the past day or so, Facebook still has a long way to go before it can bask in its previous glory.

While Facebook may be at least beginning to work its way out of the woods financially, it still has some music to face legally. Government agencies from the United States and all over the world are poised to regulate the company into accountability. As part of that, Cambridge Analytica whistleblower Christoper Wylie — who told *The Guardian* last month that he created what he calls "Steve Bannon's psychological warfare mindf*ck tool" that was used to accomplish the data breach that has led to Facebook's recent woes — told a committee of British parliamentarians that Facebook has the ability to listen in on users via the Facebook mobile app.

Wylie's testimony was connected to the British parliament's investigation into what part Cambridge Analytica played in swaying the Brexit vote. Wylie left the company in 2014, but still has an insider's view of what both his former employer and Facebook have the capability to do.

When asked by one member of parliament about the "speculation" that "Facebook can, through the Facebook app on your smartphone, listen in to what people are talking about and discussing and using that to prioritize the advertising as well," Wylie said the audio apps can capture data from the microphone in mobile devices and are able to be used "for environmental context," adding, "So if, for example, you have a television playing versus if you're in a busy place with a lot of people talking versus a work environment." He clarified, "It's not to say they're listening to what you're saying. It's not natural language processing. That would be hard to scale." He went on to say that the ability for advertisers to "understand the environmental context of where you are" would help them "to improve

the contextual value of the ad itself" since the ads companies would want to display would vary depending on where you are and what you are doing. "There's audio that could be useful just in terms of 'are you in an office environment, are you outside, are you watching TV?'"

And while Wylie seems confident that it "would be hard to scale" the ability for Facebook to be "listening to what you're saying," he is mistaken. In fact, the evidence — both anecdotal and empirical — says the company not only *can* listen to your conversations, but *is* listening. To be clear, the anecdotal evidence suggests that Facebook *is* listening and the empirical evidence shows the company *can*. So, Wylie is wrong on this point.

An article from Digg from October 30, 2017 lists several examples of the anecdotal evidence, including a video of a couple tricking the Facebook app into displaying ads for catfood by discussing — in the presence of their phones — their need to buy cat food. The couple has never owned a cat and did not do any Internet searches for cat food. And yet, though the ads they see are tailored by searches and other data collected about them, within a two-day period, they started seeing Facebook ads for cat food. Coincidence? Possibly. But the empirical evidence is not so easily dismissed.

As tech website, MakeUseOf reported in March 2016, it is not difficult to create an app that gathers real-time conversations. In fact, a couple of cybersecurity techies built one just to prove it could be done:

> To prove that other apps could be stealing data captured through your smartphone's microphone, cybersecurity expert Ken Munro developed — with the help of David Lodge from Pen Test Partners — an app that would record what was being said in the vicinity of a phone, and display it on a PC monitor.

That app was first reported by BBC. In that report, Munro explained, "All we did was use the existing functionality of Google Android — we chose it because it was a little easier for us to develop in." He went on to say, "We gave ourselves permission to use the microphone on the phone, set up a listening server on the internet, and everything that microphone heard on that phone, wherever it was in the world, came to us and we could then have sent back customized ads."

Scaling that capability to millions (or even hundreds of millions) would pose no problem for mega-tech companies such as Facebook, Google, Microsoft, and others.

One important thing Wylie added is that it's "not just Facebook, but generally other apps that pull audio" that have this capability. "Other apps that pull audio" would certainly include nearly the full suite of Google apps (Gapps) that come preinstalled on Android devices. Just consider this: For the Google voice feature to work on an Android device when a user says, "OK Google," the microphone would have to be always listening for that phrase. That means that Google would have access to that audio, and that audio includes *everything* that is within range of the microphone.

This writer uses an Android device. That device — the Oneplus 3 — has been flashed with an aftermarket version of Android called LineageOS with MicroG. That version of Android allows granular control over app permissions and does not run any Google apps — not even the "required" Google Play Services. However, this writer's wife uses an older Android device manufactured by Samsung for which MicroG is not available. On multiple occasions, she has had conversations on that phone where one or the other party says something such as, "I'll be there at 2pm" only to have Google calendar set an event with that person for that time. We have disabled all voice settings, only to have them turned back on automatically. Then the automatic calendar events start all over again.

In fact, while Google *sort of* denies this, the company also *sort of* admits it. You can even see (and hear) everything Google has on you by clicking here, if you are signed into your Google account. The tab for Voice and Audio Activity should make for some interesting listening. Seeing (and hearing) is believing; in light of this, Google's *sort of* denials don't hold much water. The company is certainly capturing audio from your microphone.

Of course, Google Home does the same thing, just without the mobile convenience.

Apple's iPhone voice search feature, Siri, works similarly. The main difference is that whereas Google makes the recorded audio available for users to hear and even delete, Apple does not. That should concern iPhone users; that even Google is more transparent than Apple is a stern indictment of the latter.

That Microsoft could be doing this is a foregone conclusion. As this writer reported in August 2015, Windows 10 is essentially spyware masquerading as an operating system. The underlying software is designed to spy on users and report back to Microsoft. Cortana's voice feature behaves suspiciously like "OK Google." Listening for a key phrase is the same as always listening. The Microsoft Privacy Agreement (which, ironically, begins by saying, "Your privacy is important to us.") says:

> To help Cortana better understand the way you speak and your voice commands, speech data is sent to Microsoft to build speech models and improve speech recognition and user intent understanding. If you choose to sign in, the speech models will become more personalized.

It's understandable if you don't remember agreeing to that: It's buried in the middle of the Microsoft Services Agreement and its accompanying documents. Those documents span some 40,000 words and would run 110 pages if printed.

Besides Facebook, Google, and Microsoft having the capability (and vested interest in the form of advertising revenues) to listen in on your private conversations, there is the whole panoply of devices known as the "Internet of Things" (IoT). Amazon's Echo with "Alexa" is always listening for commands. So it is no different. SmartTV's are not only always listening, but with integrated cameras, they are also always watching.

So, Facebook — though clearly guilty — is far from alone in this. Those concerned about privacy should certainly consider joining the growing #DeleteFacebook crowd, but they should also take a good, hard look at the other services and devices they use.

Image: Clipart.com