How Google Voice and AI Can Interfere in Users' Privacy

In the modern age of the Internet of Things (IoT), life is made easier for everyone by being connected to the Internet. But the convenience the IoT provides has another, darker, side.

In this darker side, hackers and criminals make a living out of finding and exploiting vulnerabilities to invade users' privacy. Things have gotten so bad that cybersecurity experts project cybercrime damages to reach US $6 trillion annually by 2021.[1]

Another, albeit less serious, threat users face is advertising technology (ad tech). This is the technology used by organizations and websites to track online habits. They employ tracking cookies and pixels that track online activity long after users have navigated away from their site.

Finally, there is the privacy threat posed by governments. It is already a well-known fact that some governments are spying on people.[2]

Why do people not do anything about this? Truth be told, most people take a passive approach toward their own privacy.

Communications

The first vulnerability is made up of a plethora of different media. These communication media can be classified into four basic types: calls, texts, chats and emails.

Ordinarily, calls are made through traditional landlines or mobile phones. However, with the emergence of improved technology, making calls over the Internet is possible—and this is where the problem looms.

Most applications (apps) that allow calls using the Internet are unencrypted. This means that anyone who has intercepted the signal can, therefore, listen to what should be a private conversation.

Furthermore, there has been a recent upsurge in telephone apps such as Google Voice,[3] Tetra[4] and Otter[5] that allow users to record and review all the transcribed calls they made.

As with all quality-of-life apps, this ability to record and review all calls is a double-edged sword. It provides users with more convenience, but it also exposes their privacy and information to data breaches.

Text and chat messaging apps such as Facebook Messenger and Skype create a predicament that is similar to Internet calls in that they are also usually unencrypted and, therefore, easily readable by anyone who intercepts the signal. These come with the added issue of being readable by default, unlike a call, which needs transcription.

The last vulnerable medium of communication is email. This vulnerable medium is especially infamous for being the target of many a hacker.

Many hackers have actually switched their targets from computers to humans.[6] This is because humans are easier to fool.

John Mason
Is an avid cybersecurity and online privacy enthusiast. He is the founder of and chief researcher at TheBestVPN.

Most email-based attacks are executed through phishing and its variants.[7] This is where hackers utilize psychological strategies to get users to click on malicious links that contain malware. In fact, it has been found that 92.4 percent of malware is delivered through emails[8]—that is nothing to dismiss.

Phishing aside, newer, more dastardly tactics have recently been revealed to the public. Bad actors can send victims an email with a link that stealthily turns their computers into cryptocurrency mines.[9]

Wi-Fi, Browsers and Search Engines

Web browsers, Wi-Fi networks and search engines are by far the most common privacy vulnerabilities.

Most hackers wage man-in-the-middle (MitM)[10] attacks by intercepting a user's Wi-Fi signal. Once intercepted, the hacker is then free to view and log any and all unencrypted information that courses through that signal. These attacks are most common in areas with free public Wi-Fi, for example, coffee shops, hotels and waiting areas.

That said, public Wi-Fi is a privacy risk even without MitM attacks. This is because a user never knows who set up the network and what data they log.

Public Wi-Fi aside, even private home Wi-Fi is not 100 percent safe. Home Wi-Fi networks are still vulnerable to KRACK attacks[11]—despite using the most secure encryption protocol, WPA2.

Internet browsers are yet another privacy vulnerability. A study has shown that Internet browsers are not 100 percent safe from malware.[12] The study shows that out of all the browsers, the top three browsers—Edge, Chrome and Firefox—proved the most secure.

That said, most Internet browsers are not set to the most private settings by default. They also keep track of a user's Internet traffic. The organizations behind these Internet browsers are not the only ones keeping track of Internet traffic, as even Internet service providers (ISPs) and websites do the same without suffering repercussions from the law.

On the subject of tracking, even search engines may be doing the same thing. This is why users may find it surprising that ads for certain items or services they searched for constantly haunt their screens despite their already having navigated away from the advertiser's home site.

Tracking Internet traffic comes easily to hackers, ISPs and websites because of the way Internet searches work.

> "THE LATEST AND PERHAPS THE MOST POTENTIALLY DANGEROUS PRIVACY VULNERABILITIES ARE ARTIFICIAL INTELLIGENCE (AI)-DRIVEN SMART ASSISTANTS."

Every time a user types in a search word or query, the Internet browser makes a request to a Domain Name System (DNS) server. This request has to initially pass through the ISP before it makes its way to the proper DNS server. Once it reaches a DNS server, the latter searches through all the domain names on its list of IP addresses until it finds the correct IP address.

The websites visited also place cookies in the browser. These cookies do many things, including keeping track of the items in an online shopping cart or remembering the preferences chosen for a site. However, these cookies can also track Internet traffic.[13]

AI Assistants

The latest and perhaps the most potentially dangerous privacy vulnerabilities are artificial intelligence (AI)-driven smart assistants. These AI devices not only know what the organization deploying them knows, but they also learn by themselves.

These AI assistants keep waiting and listening for users to say keywords or phrases that activate them. They start recording the user's query once they hear the keyword or phrase. This recording is then sent to the servers of the enterprise that deploys them.

While the AI assistant is waiting for its servers' response, it analyzes the query itself. If it determines that the query is something it can do locally, such as turning on the lights or muting the music, it does so without the need for further instructions from its servers. It is only after it determines that it cannot do the query locally that it waits for the servers' response before it continues.

Once a query reaches the enterprise servers, an algorithm matches it with a list of known keywords and searches for the nearest or most similar keyword. It is basically matching the query to the command that it believes the user asked. These algorithms are not perfect, though, which is why sometimes they respond with "Did you mean ___?" or "I'm sorry. I can't do that yet."

Smart assistants themselves can come with bugs that could cause a privacy breach if not found.

> "BAD ACTORS MAY EVEN ACCESS ALL THE DATA ON SMART DEVICES BY GAINING ACCESS THROUGH A MALWARE-INFECTED LAPTOP."

In one case, a journalist discovered that his smart assistant had been recording sounds around the room despite him not even saying anything. He found that even tapping the wall beside it would make it start recording. The manufacturer acknowledged the fact that their device's top button (which can also be used to initiate the device) would sometimes register "phantom touches," leading the manufacturer to remove this function.[14]

This presents a problem as there may be some conversations that users would rather keep behind closed doors. This becomes especially worrisome for users who are lawyers or medical professionals giving confidential professional advice to a client or patient and, most especially, for journalists or whistle-blowers.

Specialized devices are not the only way that AI can jeopardize users' privacy. In fact, the first AI assistants came in the form of Siri—the smart assistant developed by Apple. Some smart assistants come built into messaging platforms, such as Google's Allo and Facebook's Messenger. These AI platforms wait on every word of a conversation and come up with the best responses to the other person's message.

Another possible privacy issue is misuse. A smart home assistant acts as a hub for other smart devices in a home. It can access the door, lights, sound system and television if users allow it—and this is where things can get problematic.

The device does not know which voice it should follow and which voice it should not. This is why a child may be able to make some unwarranted online purchases. This vulnerability in home assistants was even exploited by a parrot who ordered gift boxes through Amazon's Alexa.[15] Some ads have even been known to exploit this vulnerability to prolong their message long after they have been on screen.[16]

A more serious situation arises when burglars trick a smart home assistant into opening the front door.[17] They can do this without alerting users by using an ultrasonic speaker.[18]

Bad actors may even access all the data on smart devices by gaining access through a malware-infected laptop. These hackers could gain access to credit cards or bank information once a user has made purchases using a smart home assistant. They could also peer into a home if the smart devices have cameras built into them.

Perhaps the biggest threat to privacy is that posed by governments themselves. The US National

Security Agency (NSA) can wiretap smart devices to spy on conversations. Couple this with the fact that individuals' voices can be used to profile them,[19] and this means that they can find users wherever they are in the world from even the most minute information. The NSA has spied on people before, so it is not far-fetched to say that it may be doing it now. The US Federal Bureau of Investigation (FBI) has even asked Amazon to hand over audio data that may have been recorded by an Amazon Echo near a hot tub in a murder scene.[20] The FBI may have already been spying on private conversations for years through cartapping, which is basically the act of spying on people's cars through their built-in Internet-connected devices.[21]

The NSA may be the most infamous example of mass surveillance through Internet-connected devices, but other governments have been linked to it as well. Germany was known to have used the US PRISM program (the same program used by the NSA) to aid in its operations in Afghanistan.[22] Mexico, in response to its finding out about PRISM, entered into agreements with IBM and Hewlett Packard to develop its own data-gathering software, which focused on social media and emails.[23]

What to Do About It

Users should determine if the mobile phone or messaging app they are using has a private mode or encrypted mode. Turning on this mode will prevent others from listening in or easily reading the transcripts of conversations. Facebook recently stated that no one can see encrypted messages—not even the organization behind it.[24]

Turning on encryption does mean giving up the convenience offered by the AI assistant waiting on a conversation. This is the price paid to ensure privacy.

Next, users should use a fake email, especially for unsecured sites. If a site is unsecured, it will not have a green padlock and "HTTPS" before the URL. On that note, never trust public Wi-Fi and never access sensitive accounts—online banking, emails, social media—while on public Wi-Fi without an active VPN.

> "TURNING ON ENCRYPTION DOES MEAN GIVING UP THE CONVENIENCE OFFERED BY THE AI ASSISTANT WAITING ON A CONVERSATION."

It is important to use only the strongest encryption protocol possible on home Wi-Fi. This is currently WPA2—although it is still vulnerable to KRACK attacks. WPA3 was officially announced in 2018, but it is not required just to avoid KRACK attacks. Just remember to regularly install software updates when they become available.

Perhaps the best action to take is getting the best VPN. This software provides an extra layer of protection against KRACK and MitM attacks. A VPN hides Internet traffic by masking the IP address and encrypting web activity. This encryption prevents hackers and ISPs from reading the data being transmitted and hiding the IP prevents websites, ad companies and bad actors from tracing users' identities via IP addresses.

Another way to boost the protection provided by the VPN is by foregoing the popular Internet browsers and using Tor.[25] This browser wraps data in at least three layers of encryption and makes data "hop" through the IPs of other users three times before data reach the intended server. This means that data receive the utmost privacy on their journey through the Internet.

Users who couple VPN and Tor with a privacy-oriented search engine such as DuckDuckGo[26] are well on their way to improved privacy and security from hackers, ISPs, ad companies and even spies.

Last, and perhaps both the easiest and most difficult option, users can forego using any AI-driven device or service permanently. This is easy because all that is required is avoiding anything with AI. But, this is also what makes this choice so difficult as AI assistants make modern life easier and more convenient.

Whichever of these steps are followed, it ultimately boils down to what users value most: their privacy or convenience.

At the enterprise level, employees who bring their own devices can be required to always have messaging encryption active, especially when dealing with enterprise business. If the organization instead requires the use of organization-issued devices, such devices can be preconfigured to use private messaging applications.

> “WHICHEVER OF THESE STEPS ARE FOLLOWED, IT ULTIMATELY BOILS DOWN TO WHAT USERS VALUE MOST: THEIR PRIVACY OR CONVENIENCE.”

A network firewall should be up at all times, and employees who are allowed to work while away from the premises should be required to use devices with an organization-trusted VPN service. Private email companies also offer their services at an enterprise level, so this could be a viable option for employees’ work email addresses.

Finally, to protect against KRACK attacks, organization Wi-Fi usage rules should be amended to include mandatory use of organization-trusted VPN services even when connected to wireless networks on the premises. Also, patches and updates to access point software should be closely monitored and promptly installed.

Similar to the issues users must consider when deciding how to protect their privacy, an organization’s use of any of these suggestions, ultimately, depends on the organization’s policies and data protection requirements in its jurisdiction.

Endnotes

1 Morgan, S.; “Cybercrime Damages $6 Trillion by 2021,” *Cybersecurity Ventures*, 16 October 2017, *https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/*

2 Matney, L.; “Uncovering ECHELON: The Top-Secret NSA/GCHQ Program That Has Been Watching You Your Entire Life,” *TechCrunch*, 2015, *https://techcrunch.com/2015/08/03/uncovering-echelon-the-top-secret-nsa-program-that-has-been-watching-you-your-entire-life/*

3 Karch, M.; “What Is Google Voice?” *Lifewire*, 4 May 2018, *https://www.lifewire.com/what-is-google-voice-1616888*

4 Sawers, P.; “Tetra’s Call Recorder and AI-Powered Transcription App Now Works for Inbound Calls,” *Venture Beat*, 20 February 2018, *https://venturebeat.com/2018/02/20/tetras-call-recorder-and-ai-powered-transcription-app-now-works-for-inbound-calls/*

5 Perez, S.; “Otter’s New App Lets You Record, Transcribe, Search and Share Your Voice Conversations,” *TechCrunch*, 2018, *https://techcrunch.com/2018/02/26/otters-new-app-lets-you-record-transcribe-search-and-share-your-voice-conversations/*

6 Zurkus, K.; “Hackers Prey on Human Resources Using Ransomware,” *CSO*, 29 August 2016, *https://www.csoonline.com/article/3112855/technology-business/hackers-prey-on-human-resources-using-ransomware.html*

7 Rashid, F.; “Types of Phishing Attacks and How to Identify Them,” *CSO*, 27 October 2017, *https://www.csoonline.com/article/3234716/phishing/types-of-phishing-attacks-and-how-to-identify-them.html*

8 Verizon, *2018 Data Breach Investigation Report*, USA, 2018, *https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf*

9 Nadeau, M.; “What Is Cryptojacking? How to Prevent, Detect and Recover From It,” *CSO*, 29 August 2018, *https://www.csoonline.com/article/3253572/internet/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html*

10 GlobalSign, “What Is a Man-in-the-Middle Attack and How Can You Prevent It?” 1 March 2017, *https://www.globalsign.com/en/blog/what-is-a-man-in-the-middle-attack/*

11 Krackattacks.com, “Key Reinstallation Attacks,” *https://www.krackattacks.com/*

12 Pathak, J.; T. Skybakmoen; “Web Browser Security Comparative Report,” NSS Labs, 1 November 2016, *https://www.nsslabs.com/research-advisory/library/endpoint-protection/web-browser-security/web-browser-security-comparative-report-sem-protection/comparative-report-web-browser-security-socially-engineered-malware-protection/*

13 Hill, S.; "How Much Do Online Advertisers Really Know About You? We Asked an Expert," *Digital Trends*, 27 June 2015, *https://www.digitaltrends.com/computing/how-do-advertisers-track-you-online-we-found-out/*
14 Russakovskii, A.; "Google Is Permanently Nerfing All Home Minis Because Mine Spied on Everything I Said 24/7 [Update x2]," *Android Police*, 10 October 2017, *https://www.androidpolice.com/2017/10/10/google-nerfing-home-minis-mine-spied-everything-said-247/*
15 Greatrex, C.; M. White; "Parrot Manages to Fool Amazon's Alexa and Orders His Own Gift Box Without His Owners Knowing," *Mirror*, 20 September 2017, *https://www.mirror.co.uk/news/uk-news/parrot-manages-fool-amazons-alexa-11207953*
16 Diaz, A.; "The Whopper Lives! BK's 'Connected' Ad Triggers Google Home Once Again," *Ad Age*, 13 April 2017, *https://adage.com/creativity/work/burger-king-connected-whopper-v-3/51514*
17 Weisbaum, H.; "'Hey Alexa, How Secure Are Voice-Activated Assistants Like You?'" NBC News, 28 November 2018, *https://www.nbcnews.com/tech/security/hey-alexa-how-secure-are-voice-activated-assistants-you-n824566*
18 Song, L.; P. Mittal; "Inaudible Voice Commands," 24 August 2017, Princeton University, New Jersey, USA, *https://arxiv.org/pdf/1708.07238.pdf*
19 Capital Flows, "Voice Recognition: Risks to Our Privacy," *Forbes*, 6 October 2016, *https://www.forbes.com/sites/realspin/2016/10/06/voice-recognition-every-single-day-every-word-you-say/#19368ea6786d*
20 Brandom, R.; "How Much Can Police Find Out From a Murderer's Echo?" *The Verge*, 6 January 2017, *https://www.theverge.com/2017/1/6/14189384/amazon-echo-murder-evidence-surveillance-data*
21 Brewster, T.; "Cartapping: How Feds Have Spied on Connected Cars for 15 Years," *Forbes*, 15 January 2017, *https://www.forbes.com/sites/thomasbrewster/2017/01/15/police-spying-on-car-conversations-location-siriusxm-gm-chevrolet-toyota-privacy/#7e9dd7c22ef8*
22 *Spiegel Online*, "Bundeswehr soll schon 2011 von Prism gewusst haben," 17 March 2013, *www.spiegel.de/politik/deutschland/bild-bericht-bundeswehr-soll-von-prism-gewusst-haben-a-911531.html*
23 Villamil, J.; "Big Brother y CISEN, millonario negocio en puerta," proceso.com.mx, 18 June 2013, *https://www.proceso.com.mx/345205*
24 Johnny 5, "Facebook Finally Stands Up for Privacy as the US Government Demands to Hack Messenger," ExpressVPN, 28 August 2018, *https://www.expressvpn.com/blog/facebook-stands-against-government-demands-to-hack-messenger/*
25 Tor, "Want Tor to Really Work?" *https://www.torproject.org/download/download.html*
26 DuckDuckGo, *https://duckduckgo.com/*