Which Investigates S2 - EP5 v4

[00:00:00.15] - I don't know about you, but I love a good spy movie.

[00:00:03.36] [JAMES BOND THEME MUSIC]

[00:00:07.10] Yeah, I enjoy the gratuitous action sequences, that obligatory rooftop motorcycle pursuit. But for me, it's more about the spycraft, the almost believable gadgets, the expertly executed heist.

[00:00:20.12] [AUDIO PLAYBACK]

[00:00:20.51] - You're only supposed to blow the bloody doors off.

[00:00:23.80] [END PLAYBACK]

[00:00:24.08] - As always though, facts can be as Oscar-worthy as fiction.

[00:00:27.91] [MUSIC PLAYING]

[00:00:31.06] It's been said that during the Cold War, there were more listening devices than employees in the US embassy in Moscow. And some were brilliantly hidden. Journalist Robert Lucky tells of a bugged typewriter, where a solid aluminium bar-- part of the structural support of the typewriter-- had been replaced with one that looked identical. And it was repurposed along with some springs and screws to act as an antenna. You've got to hand it to the Soviets. That is some impressively sneaky surveillance right there.

[00:01:01.57] And we were doing much the same over in Britain too. In 1956, a Special Agent disguised as a telephone technician gained entry to the Egyptian embassy in London and installed a hidden microphone. And it's no coincidence that shortly after, Britain launched an attack on Egypt in what became known as the Suez Crisis. And of course, across the pond, presidents were signing off on countless surveillance missions. In the 1970s, President Richard Nixon's administration bugged almost every US government department-- including the Oval Office itself. Remember Watergate, anyone?

[00:01:41.02] Using spy-like gadgets and hidden bugs to overhear secrets-- it feels like a thing of the past. But it's very much still a thing of the present. But listening devices though, they no longer need to be covertly placed. They're there in the devices that we carry around with us. And we're now welcoming more of them into our homes. Alexa, how was your day?

[00:02:02.41] - It's been super productive. I set a gazillion timers. And now, I'm brushing up on my [INAUDIBLE].

[00:02:07.90] [MUSIC PLAYING]

[00:02:12.72] - According to research done this year by Ampere Analysis, over half of UK homes with an internet connection now have a smart speaker with a voice assistant device-- a higher percentage, in fact, than the US. They set alarms. They play music. They tell us whether we should take an umbrella out today.

[00:02:30.54] But they're also the motivation for one of your most asked tech and security questions. In a Which survey-- conducted especially for this podcast-- when asked about smart speakers, 76% of respondents said they were concerned about their privacy. Should you be? I am Greg Foot. And this week's Which Investigates asks, hey, Google, is your smart speaker always recording what you say?

[00:02:54.80] - (COMPUTER VOICE) Your audio recordings are not being saved with your assistant history.

[00:02:58.41] - Hmm.

[00:02:58.83] [MUSIC PLAYING]

[00:03:18.50] Which Investigates is a podcast from the UK'S consumer champion. We work to make life simpler, fairer, and safer for everyone. In this season, I'm exploring concerns around tech and security. Are you being tracked online? How hackable is your own home? Is technology helping the scammers? If you've got something you'd like us to investigate, do get in touch. If you're on social media, I am at Greg Foot. And Which is at Which UK. Or you can email us on podcasts@which.co.uk.

[00:03:47.11] [MUSIC PLAYING]

[00:03:54.21] [MUSIC PLAYING]

[00:03:56.11] Coming up, I get to the bottom of how these devices work.

[00:03:59.62] - If you want to ask Alexa something, or Siri something, or Google something, they're listening out for you to say the wake words. So it's listening for hey, Google, or Alexa, or hey, Siri. It's not listening beyond that until you literally tell it to do so by using its wake word.

[00:04:16.39] - I get a wake-up call, when one of my expert guests-- whose research is all about smart speakers-- says this.

[00:04:22.99] - The reason that I don't have one is, personally, there are just too many unknown privacy and security consequences at the moment to having these devices.

[00:04:32.74] - And it becomes clear that if the main privacy concern is about surveillance, we should be looking much further than just the smart speaker in the corner.

[00:04:41.93] - A bunch of devices listen to sounds. Certainly your phone, your computer-- they all have microphones. Any smart device that you give voice commands to has a microphone. And these all listen to us in different ways, at different times, for different purposes. But there's a lot in our environment that is listening.

[00:05:00.69] [MUSIC PLAYING]

[00:05:05.58] - As I mentioned in the first episode of this tech and security season of Which Investigates, the smart gadget boom over the last decade has been huge. According to research carried out in April this year by energy comparison website USwitch, the pandemic

saw British consumers spend a whopping $33 billion pounds on smart gadgets-- an average, they say, of 640 pounds per household over the past year. And of the 2,000 UK adults surveyed, over a quarter had picked up a smart speaker.

[00:05:36.63] Maybe, like me, you have an Amazon Echo speaker with Alexa-- the current market leader in voice assistant technology. Or you might have Google's Nest speaker with Google Assistant on it. I don't know about you, but whenever I use one, I feel like I'm living in the future. But the history of voice assistant technology goes back many decades.

[00:05:56.96] [MUSIC PLAYING]

[00:06:00.32] In 1961, around the time the US embassy in Moscow was riddled with those listening devices, IBM launched the predecessor of the smart speaker that we have in our homes today. It was called the shoe box. And it could recognise a whopping 16 words. That number didn't increase to 100 recognised words until 10 years later, thanks to a new device from Carnegie Mellon. And if you're wondering how many words Amazon's Alexa now understands, it is tens of thousands of words in nine different languages.

[00:06:33.92] [MUSIC PLAYING]

[00:06:36.28] In the 1990s, Microsoft brought users a different type of assistant. Not a physical one, but a digital one-- Clippy. Who remembers Clippy? Not me. I'm obviously way too young. No, I definitely remember it. Clippy was a paper clip based character who asked users if they needed help-- guiding newbies around the platform.

[00:06:58.09] Depending on who you ask, Clippy was either the most useful thing ever or the most annoying thing ever, especially as you couldn't turn it off. Five years later-- 1996-- Microsoft added speech recognition software to its office suite. Gone were the days of typing out an essay. But the AI software was patchy, to say the least. And yeah, we still type.

[00:07:21.93] [MUSIC PLAYING]

[00:07:25.21] Then in 2011, along came Siri.

[00:07:27.76] [SIRI BEEP]

[00:07:28.45] Three months later, Google tried to follow suit with Google Now. Remember that? No. Me neither. Then, in the years that followed, Microsoft's Cortana arrived. Then Amazon's Echo, and the real game changer, Alexa, as well as Google Home-- now Nest-- which solidified the dominance of smart speakers in the market. But how does this latest voice assistant technology actually work?

[00:07:51.65] - So generally, smart home assistants are always on. And they are hearing for wake words and followed by commands that we give to them. Whether it's turning on a light bulb or playing a song and things like that. So in general, the data that they collect usually is audio snippets from our conversations and commands that follow those wake words.

[00:08:12.22] - This is Hamed Haddadi, reader in human centred systems at Imperial College London. And as you'll hear today, there isn't much about voice assistants that he doesn't know. Let's address these wake words first then. What are they, and why are they important?

[00:08:27.07] - My name is Kate Bevan, and I'm the editor of Which Computing Magazine.

[00:08:30.76] - If you listen to the first episode of this season, you've already met Kate. And you'll know that she's got a fair few smart devices in her home.

[00:08:37.21] - If you want to ask Alexa something, or Siri something, or Google something, they're listening out for you to say the wake words. It's listening for, hey Google, or Alexa, or hey, Siri. It's not listening beyond that until you literally tell it to do so by using its wake word.

[00:08:53.92] - I'm sorry, this episode should have come with a warning, shouldn't it, at the start that we would be waking up any smart devices that can hear this audio. Whoops.

[00:09:01.42] - Technically, there is a microphone on the device, which is always on and it's always listening. However, it's not always transmitting.

[00:09:08.84] - So it is always listening for those wake words. And it doesn't sound like it's always recording. But how long does it record for, and can it record bits you don't want it to record? Those questions on the way. Because first, what happens to the recording of what you say after you've said the wake word?

[00:09:28.75] - What happens is that the audio snippet gets sent to the cloud provider, which then does speech to text conversion, looks at the content of the audio and the specific command that you are giving to it, and takes an action based on that.

[00:09:42.68] - And here is something that I had no idea you could do until I started researching all this.

[00:09:47.02] - Legally, they have to provide you with the option of accessing all of the recording snippets that they have available from you. Yes. Under GDPR regulations, you are legally entitled to ask these smart speaker providers for the transcripts of your audio recordings. And you can then delete one or all of them.

[00:10:04.67] So let's see what mine has recorded, shall we? I've got multiple Amazon Echoes around the house. So I'm going to go to amazon.co.uk/Ale xaprivacysettings. Then review voice history. Regardless of which device you own, it's pretty much the same process. While I'm doing this, I'm going to give producer Robert a call.

[00:10:25.45] [PHONE RINGING]

[00:10:30.22] - Hello, buddy.

[00:10:31.00] - Hello. Hello.

[00:10:32.05] - Would you like to hear what Amazon have recorded of me speaking to Alexa?

[00:10:35.77] - There are very few things I would like to do more. I'm very excited about it.

[00:10:40.81] - All right. Hang on. Hang on. Hang on. Here's one at 8:32 in the morning.

[00:10:45.64] - What's the weather like today in London?

[00:10:48.04] - Very good. A very good way to start the day. You need to know the answer. Yeah, why not?

[00:10:53.53] - Didn't want to get wet, did I? Needed to know if I need to take an umbrella. Hang on. I'll give you a classic from yesterday. Here was yesterday evening's.

[00:11:01.42] - Alexa, lamps on.

[00:11:03.10] - Wow, as far as weeknights go in the Foot household, that's pretty exciting, isn't it?

[00:11:07.43] - And then, later on,

[00:11:08.77] - Alexa, lamps off.

[00:11:10.66] [LAUGHTER]

[00:11:12.58] - Great to hear that you are really using all of the capabilities of your smart speaker.

[00:11:18.52] - It's actually really boring. There are a lot of turn on timer for 10 minutes, or well, it's lights on, lights off the whole blooming time.

[00:11:26.17] - I'm guessing as well that when you're doing the whole lights on lights off thing, the switch isn't far away, is it? Let's be honest.

[00:11:31.66] - Yeah. OK, fair enough. Yeah. But as I've already said, I feel like I'm in the future if I ask for the lights to be turned on by some mystery voice in the corner.

[00:11:40.31] - It is pretty cool. It is pretty cool. It makes you, like you say, you feel a bit like you're in Blade Runner or something like that.

[00:11:46.28] - So here's an interesting one. This one says, from the other day, at nine o'clock in the morning, it says, audio was not intended for Alexa. But I can still play it. Here you go.

[00:11:56.00] [BANGING]

[00:11:56.45] - Alexa.

[00:11:58.25] - What was that?

[00:11:59.30] - So that sounded like probably me putting pots and pans away or like emptying the dishwasher.

[00:12:03.95] [BANGING]

[00:12:04.93] - Alexa.

[00:12:06.40] [LAUGHTER]

[00:12:06.89] - There is kind of an Alexa-ish noise at the end, but I don't think00 that's not me saying it. So that might have been picked up off a podcast or the radio.

[00:12:17.13] - Weird.

[00:12:18.13] - Hmm. Here's the recording on the one that's in the lounge of when I was just recording this podcast just now. And I said, Alexa, how is your day?

[00:12:26.60] - Alexa, how is your day?

[00:12:29.33] - So you can hear how far away it is. That's through a wall and through a door.

[00:12:33.80] - I think you need to get on to the people that soundproofed your downstairs cupboard and tell them that they need to come back and do a better job.

[00:12:40.77] - Yeah. That was just me. Me and some insulation panels off the internet.

[00:12:45.11] - Have a word with yourself, then.

[00:12:46.29] - Have a word of myself. So Rob, knowing that I would be recording this this afternoon, I thought I'd have a bit of fun this morning with Alexa. So I've recorded a couple of things for you.

[00:12:55.28] [LAUGHTER]

[00:12:56.90] - Is this your gift?

[00:12:58.40] - Just to see. I just wanted to test what happened. All right. Here you go.

[00:13:02.60] - Alexa, what's the weather like in London? And here's some top secret information that we're now speaking about straight after this. I'm also rustling a beanbag. How much of it delivered?

[00:13:11.54] [LAUGHTER]

[00:13:12.98] - Now, I see what you're doing there.

[00:13:14.27] - Yeah?

[00:13:14.72] - And it kind of worked.

[00:13:16.21] - Yeah? Yeah. I was saying, oh, I think you could pick it up. I think it was quite clear. I was saying, Alexa, what's the weather like in London? But then rather than pausing afterwards, I instantly turned to the next thing. And I said, and here is some top secret information that I'm now speaking about straight after this whilst rustling-- this is the key-- whilst rustling a beanbag, so there wouldn't be that moment of pause.

[00:13:38.24] - And it just keeps it going, doesn't it? It doesn't turn off the recording.

[00:13:41.90] - But it didn't take the whole of my line. Because I think at the end I said, and I wonder how much it is recording. Or how much of this did it record. And it stopped just before the end of that.

[00:13:50.86] - Let's have it again. Play it to me one more time.

[00:13:52.52] - Alexa, what's the weather like in London? And here's some top secret information that we'll now speaking about straight after this, whilst rustling a beanbag. How much of it did it--

[00:14:01.70] - Oh. So it's almost like Alexa knew it was doing wrong.

[00:14:04.85] [LAUGHTER]

[00:14:05.06] - But it still got some of it.

[00:14:07.76] - And then, this is one I just thought I would see if I had spoken to Alexa, just to say, stop. To stop playing the radio this morning. And then, spoke to a different smart assistant. I went for Siri, with a message that I wouldn't want anyone to record.

[00:14:22.85] - Stop. Siri, ring James Bond. I need to tell him about his latest mission. Don't tell anyone else though.

[00:14:30.05] - There was even a pause. There was a pause after stop as well.

[00:14:33.06] - Firstly, it's nice that you can just have a conversation with all of your smart speaker friends in the kitchen, in place of actual normal human beings. That's nice.

[00:14:40.97] - Go and entertain myself. But there's an example. If those were bank details that I was reading out, I'd said, Alexa, stop. There was a little pause. And then, if I then started reading out bank details because I was on the phone or something, that could have recorded it.

[00:14:54.02] - And it felt like that pause was long enough that it should have stopped.

[00:14:58.91] - Here it is again.

[00:15:00.08] - Stop. Siri, ring James Bond. Need to tell him about his latest mission. Don't tell anyone else.

[00:15:06.74] - I reckon you've got at least half a second there.

[00:15:08.70] - Yeah, there's a little pause. So that was a good example of it not stopping recording when you want it to.

[00:15:15.53] - Interesting. I mean, like you said, you could then pick up all sorts of stuff.

[00:15:21.08] - You absolutely could. All right, we'd better get on with the podcast, actually, hadn't we?

[00:15:24.86] - Much love. Bye-bye.

[00:15:26.02] - [INAUDIBLE]

[00:15:26.45] [MUSIC PLAYING]

[00:15:31.88] - I asked Kate at Which if she, as a big user of smart devices and voice assistance, checks her recordings.

[00:15:38.06] - I don't do it routinely, because actually, when I go and look at my logs, it's really mundane. It's Alexa, turn on this light, or Google, set a timer. But yes, if you're concerned about it, or you think it might have woken up inadvertently, and if you've got a friend with a name that's similar to the wake word-- like I've got a friend call Lexi. And sometimes if I'm talking to her, Alexa perks up and starts listening. So if something like that's happened, or even if you're just concerned, go back and have a look at it. And you can delete what's there.

[00:16:07.25] - So far so good, I guess. Yes, they are always listening. No, they're not always recording. The bits they record are pretty much all boring. You can regularly delete them if you want to. Sometimes they do record more than you think they're recording. And then, I spoke to Hamed, an expert in all these technologies. I asked him if he has one. And he said this.

[00:16:30.32] - Do you have one?

[00:16:31.22] - I don't. No. I don't have a home assistant.

[00:16:33.53] - And why is that?

[00:16:34.58] - I think at the moment the risks that are associated with them outweighs the actual service that they provide. There are just too many unknown privacy and security consequences at the moment to having these devices.

[00:16:47.63] - Well, there you go. Unknown privacy and security consequences. And Hamed isn't alone with these concerns. In a 2020 paper entitled "Unacceptable-- Where is My Privacy?" researchers at Ruhr University in Bochum, Germany analysed something they called accidental triggers-- i.e. Sounds that should not have triggered the voice assistant to start transmitting and likely recording, but did.

[00:17:10.97] They found more often than not, that these triggers unsurprisingly came from words or phrases similar to the preset wake words. They said, a lesson was found to prompt Alexa into action. OK cool could wake Google. The researchers even found two triggers that weren't caused by speech at all. There was a ringing phone in the TV show New Girl that triggered Amazon's Alexa, as did a honk made by a car horn in The Simpsons.

[00:17:37.34] On Amazon's own information page entitled, Is Alexa Recording? They say, quote, "On some occasions, Alexa may accidentally wake up when the wake word wasn't spoken. But your echo device thought it was." For example, you're talking to a friend. And you say, I saw on the news that we elect a new Senator this year. There is a small chance that your Echo device may incorrectly identify elector as the wake word Alexa.

[00:18:03.23] Then they say, "bracket, that's getting better, by the way. We are constantly improving our wake word detection technology," end quote. The worry then, is what could be inadvertently recorded after an accidental trigger? And this is something that we've tested here at Which.

[00:18:18.46] [MUSIC PLAYING]

[00:18:20.83] - Hi. I'm Oliver [INAUDIBLE]. And I am responsible for testing many types of audio products at Which, including smart speakers. We had a lot of concerns from people that these devices might be collecting too much information about people. We didn't just want to ask the manufacturers. We wanted to check for ourselves. We got six volunteers. And we got six different smart speakers. And we asked each of them to take one of them home and use them naturally, just as a normal consumer would, and see how they got on with them.

[00:18:49.36] And we also asked them to give the speaker some testing questions that we pre-prepared in advance, just to see whether we could trick the devices into doing things that you wouldn't normally expect them to do. So things like with Alexa, if you ask something very similar, like is Alex around? Alex is a very common name, of course, will it think that you said Alexa, and things like that. So we were basically trying to see what are the limits of these devices.

[00:19:15.04] - The results won't come as much of a surprise.

[00:19:17.51] - We found that both Alexa and Google Assistant recorded more conversations than we expected them to. For Google Assistant, we found that some phrases were collected even when you hadn't used the wake word, and also that some phrases that you'd said just before that wake word were also recorded. So you might have said something like, I'm just going to end my bank details. Hey, Google, and then ask a question. And it will record a little bit before, which is a little bit concerning. And we also, found that the voice assistants continued recording even after some brief pauses.

[00:19:49.55] So you might ask Alexa, what's the weather like, and then start another conversation with somebody else in the room just afterwards, and it would record both of them. And you would only expect it to record the bit that you directed at Alexa. We also found that if you stop and change your mind, so you say, Alexa, and then you decide you want to do something else-- maybe pick up the phone or something like that-- it would record what you said.

[00:20:10.93] - In March this year, the EU published privacy guidelines designed to help resolve the issue. In the report, they said manufacturers should keep users informed about what data has been stored and even suggests using technical solutions like noise philtres to stop accidental awakenings. Whether the UK will adopt these proposals and whether big tech companies will listen-- no pun intended-- well, that's another story.

[00:20:35.35] [MUSIC PLAYING]

[00:20:40.61] So Oliver just mentioned that these devices can sometimes record when we aren't expecting them to. But how long do they record for?

[00:20:47.95] - Usually, they have a maximum time, which is usually in order of 10 to 20 seconds, depending on the manufacturer. And usually, they time out after a second or so of silence.

[00:20:58.36] - So if somebody is having a conversation in the background as you ask the question, it could genuinely record for 20 seconds?

[00:21:05.56] - It could continue recording, yes. And the interesting thing is that it doesn't record then transmit. It starts transmitting while the recording is being made, in order to be able to respond faster. So yes. At a certain point, that data might have already left your home, basically.

[00:21:21.31] - And that's exactly what I found. Not only with the bean bag rustling experiment, but also after I'd said stop, pause, and then started speaking to Siri. And it was actually while I was chatting to Oliver that I had a bit of a realisation. It isn't just the voice assistants on smart speakers that we need to consider here.

[00:21:38.83] - A bunch of devices listen to sounds. Certainly, your phone, your computer-- they all have microphones. Any smart device that you give voice commands to has a microphone. And these all listen to us in different ways, at different times, for different purposes. But there's a lot in our environment that is listening.

[00:21:57.91] - This is Bruce Schneier, one of the US's leading technology and security experts. And it was brilliant to get some time with him for this podcast. More of that conversation on the way, shortly though. Because first, I'm going to hazard a guess that the very device that you're listening to this podcast on right now has a microphone. Which means it could be listening to you right now, primed and ready for a command.

[00:22:19.48] - Your phone is just this massive surveillance device. You're basically carrying tracking devices around with you.

[00:22:25.57] - This is Kate from Which again. And this notion of being tracked is what next week's investigation is going to focus on. For now, though, I had a question for Kate. Hamed told me that my interactions with the voice assistant were being instantly transmitted to the cloud, where there's an AI, I presume, doing the speech to text conversion. But do humans ever listen to those recordings?

[00:22:47.14] - Some recordings are looked at by human beings to help to build its accuracy. Google says, it's around 0.2%.

[00:22:55.87] - Google themselves have previously said that real people occasionally listen to audio snippets to improve the quality of speech recognition across search. Which I guess makes sense. You want the software to be the best it can be. And you need to test how well it's doing its thing. But if they listen to an accidentally triggered clip, or a clip that records too long, and they hear something that you wouldn't want a stranger to hear-- hmm. I mean, even more worrying was a report I read on news site Bloomberg from 2019.

[00:23:25.73] They confirmed what we've just heard, that humans are sometimes listening to improve these device's speech recognition technology. But they also revealed that some of the reviewers said that they had shared some of the funnier clips with one another in an

internal chat room. What? And others even worried that they'd heard evidence of assault being carried out. Amazon says it takes security and privacy seriously. When we contacted them for this podcast, they told us, quote--

[00:23:54.53] - We have built privacy deeply into the Alexa service. Customers talk to Alexa billions of times a month. And in rare cases, devices may wake up after hearing a word that sounds like Alexa or one of the other available wake words. No audio is stored or sent to the cloud unless the device detects the wake word. And customers will always know when Alexa is sending a request to the cloud, because a blue light indicator will appear on their Echo device. Our wake word detection and speech recognition get better every day. And we continue to invest in improving this technology.

[00:24:27.10] - But if a wake word is detected, then this audio-- as Amazon just told us-- is stored in the cloud. But what and where is that?

[00:24:35.86] - The cloud is basically somebody else's computer. So your email might be on Google's computers, or Microsoft's computers, or on Apple's computers. This is the cloud. But it's computers in a building somewhere on the planet that someone else controls. That's all the cloud is.

[00:24:52.21] - And having started this season off with a couple of episodes on hacking, I was keen to know if having my recordings in the cloud makes it easier or harder for someone to hack in and access it, especially after our own home hacking video on the Which website showed how these devices can be used to hack other devices. That's what's known as a second order attack.

[00:25:13.96] - It's hard to assign hacking probabilities. In general, the companies that run cloud services are more sophisticated than the average computer user. For most of us, our data is safer in the cloud, just because Google is going to do a better job at securing it than you are.

[00:25:33.31] - Hacking into devices is, I would say, one of the lower concerns in a way. Because usually, the good devices are provided by quite reliable and strong companies where they have a big security team looking into these things. But the problem is, that's extensive data collection.

[00:25:50.68] - Which means, it's that time in the show-- and I feel this should be a recurring thing-- when we talk about data.

[00:25:56.04] [MUSIC PLAYING]

[00:26:00.63] Seriously, though. As we'll hear in a second, access to your data is one of the main reasons that Hamed doesn't want a smart speaker with a voice assistant in his house. Long gone are the days when a listening device's main purpose was to reveal some kind of state secret or to inform warring superpowers at the other was about to launch a nuclear attack. In 2021, it's all about building up a profile of what you do and don't like-- a profile advertisers can exploit.

[00:26:28.03] - So the fact that this audio is collected could potentially lead to other information being collected from the user as well. For example, you can guess more or less

their age, their gender, their emotional status, their well-being. So at the end of the day, the majority of these devices are provided by big companies, which majority of their income is from advertising and analytics revenue.

[00:26:52.96] So they would be able to use that data to form a better profile about you and then offer that to third parties for specific adverts. Whether it's trying to nudge your voting, or your shopping behaviours, or your political interests, and things like that. And we've seen numerous examples of this in the past from the web browsing world and the mobile app world. But now we have a whole new channel of information collection.

[00:27:20.31] - And again, it's not just Hamed who is concerned about this. In a report released by US consumer group, Consumer Watchdog, they explained how they'd examined future patent applications by Amazon and Google, which they say, prove future versions of Amazon and Google's smart assistants could use our data to try and sell us products.

[00:27:39.81] - The amount of data is literally a few seconds of data that it's actually keeping. But of course, there's nothing to stop them from changing that. If you wanted to hear everything that everyone was saying, I'm sure that's probably-- you can just make that happen.

[00:27:51.66] - This is Paul Vassilis, who I spoke to for next week's tracking-related investigation. But after a great hour of talking about data and privacy and our online footprint, I quickly asked him about smart speakers.

[00:28:03.97] - You may know I do this TV show Hunted for Channel 4. And one of the things we did on one of the celebrity once was, we hacked into one of the Made in Chelsea star's Amazon echos. And we were able to see his history-- his voice history of everything he'd ever said. There were a couple of quite amusing late night drunken asking to play songs when he obviously had a few too many drinks and stuff, which was just a bit of fun. At the moment, they're not much more than toys. But as they become more significant, I think that could start to become a bit more of a worry.

[00:28:30.87] - The Consumer Watchdog report that I mentioned earlier uncovers the Amazon filed a patent application for an algorithm that could let future versions of the device identify statements of interest, such as, I love skiing, that then enables targeted advertising. And a Google patent application describes using a future release of its smart home system to monitor and control everything from screen time and hygiene habits to travel schedules and various other activities.

[00:28:57.81] - This could go toward some sort of Big Brother society, where these companies-- based on the interaction that you have with the home assistant-- they can specifically ask about your emotions and try to take actions based on the emotions that you have.

[00:29:10.83] - Hmm. That's worrying.

[00:29:12.06] - There's an entire ecosystem of data surveillance. A lot of companies profit from it. In the US at least, the market is very opaque. There are thousands, possibly 10 thousands-- we don't even know-- of data brokers that buy and sell and use your data.

Certainly the large platforms-- the Facebooks and Googles-- they make all their money spying on you. That's their business model.

[00:29:34.45] - We did contact Amazon, Facebook, and Google. But only Amazon came back to us. With regards to the patent application I just mentioned, they said, quote--

[00:29:43.17] - Like many companies, we file a number of forward looking patent applications that explore the full possibilities of new technology. Patents take multiple years to receive and do not necessarily reflect current developments to products and services. We do not use customer's voice recordings for targeted advertising.

[00:30:00.00] - Here in the UK, there are ways to find out what data company holds about you. And what's more, ways to stop companies profiting from your own personal information. For example, article 21 of the 2018 Data Protection Act allows you to make a request to an organisation to stop processing your data for the purposes of direct marketing. There's a really useful guide on how to do this on the Which website. And I'll put a link to that in the show notes.

[00:30:24.57] [MUSIC PLAYING]

[00:30:29.27] Finally then, I think it's worth asking-- are we perhaps fearing a future that might never happen? Well, here's the outcome of Which's recent investigation that Oliver mentioned earlier.

[00:30:38.92] - For the manufacturers, basically, the bottom line of this investigation was that we didn't find anything that we thought was nefarious in what they were doing. But what we did find is lots of shortcomings that we think could be improved.

[00:30:51.31] - Sounds like a school report, doesn't it. And we should balance this whole discussion with the other side of the coin-- the benefits that these devices can offer.

[00:30:59.92] - Inherently, there are benefits to these things as well. If you want to think about it, for example, for people with difficulty in mobility, or for people who are living alone, or for people who are working in the specific constrained environment, or elderly, and things like that. So these devices can be made useful.

[00:31:18.10] - Hamed's decision was that those benefits don't outweigh the potential costs. What does Kate from Which think?

[00:31:24.52] - Do you have concerns about smart assistants and what they might be recording?

[00:31:29.53] - Yes and no. I mean, yes, if you stop and think about it, it's a bit creepy to think that there are devices in your house listening out for what you say. But also, I use them myself. I've got a lot of smart home stuff and love being able to shout at the heating to come on if it's cold in the morning without having to get out of bed. I love being able to turn lights on and off and music on and off with my voice. So perhaps, I've kind of internalised it. I think increasingly, we are going to do that. And there is a trade-off. These things are more useful the more information they have about you.

[00:32:06.92] - But the more information they have about me, the more useful that data is to marketers-- or as Hamed mentions-- the more information they might have to target advertising to try to nudge my shopping behaviours or to align me with certain political interests. That line of investigation is more a circle. You end up going round and round and round. But there is one last promising report that I want to tell you about.

[00:32:29.62] [MUSIC PLAYING]

[00:32:32.92] In 2019, cybersecurity firm Wandera found no evidence that phones or apps were secretly listening to us. Researchers put two phones-- one Samsung Android, one iPhone-- into an audio room, where for 30 minutes they played the sounds of cat and dog food adverts on loop. Two identical phones were also put in a silent room. Now, the researchers kept apps open for Facebook and Instagram, Chrome's Snapchat, YouTube, and Amazon with full permissions granted to each platform. And then, they looked for adverts related to pet food on each platform and web page they subsequently visited.

[00:33:08.50] They repeated the experiment at the same time for three days. And they noted no relevant pet food adverts on the audio room phones, and no significant spike in data or battery usage either. Which means, at that time, you saw a holiday to Greece being advertised on social media after chatting to a friend about how much she'd love to visit Athens, this study suggests that is not down to your phone listening to you. And Hamed's research confirms that too.

[00:33:33.91] - There has been loads of studies-- even including our own labs-- showing that these devices are not constantly recording and transmitting data. Because that would be a lot of data. And it's just complicated.

[00:33:44.71] - However, the type of adverts you get when you say, hang on, I've never searched for this online. But I did talk about it in the kitchen yesterday-- something must have heard that to give me these adverts. They're actually down to something entirely different.

[00:33:58.43] - However, the fact that I have so much information online available from me, and the fact that I meet a friend today, and the phone can detect, for example, that I've been meeting a friend based on a number of things-- proximity of the devices, calendar invites, social media messages, and all of that, it might just be that that person actually has done a search for that specific topic or that specific thing. And I also get an ad for that.

[00:34:26.80] Or it might be that the models that are being made from us are so good nowadays, and they can take so much details, that predicting what I might need or what I might be interested in is not actually super complicated. So while it might seem to us that this specific app has been listening to me all the time, no, it's just the fact that there are so much data being collected about us that makes prediction much easier.

[00:34:49.84] - As always, it is all about the data.

[00:34:52.75] - I mean, it's entirely reasonable to worry about what your smart assistants are listening to, and what they're sending to the cloud, and what they know about you. But remember, it's not just smart assistants. The web, and Facebook, and everything else is tracking everything you do online as well.

[00:35:06.07] [MUSIC PLAYING]

[00:35:08.42] - Any time we go online, we are adding to the piles of data that companies have about us. Our every online step-- even when we think we're offline, but our phones, say, are still connected-- every step is being tracked. How that is happening-- and more on the why too-- that's the topic for next week's investigation. A kind of part two to this one, I guess.

[00:35:29.15] And I should repeat what I said earlier, there are plans afoot for the UK's data protection regulations to be reformed. That's the UK GDPR, which sits in the 2018 Data Protection Act. The GDPR was a European-wide Data Protection Regulation which the UK adopted. We still adhere to it until 2025. But now, we are, of course, outside the European Union. And the government are considering widespread change. It's one to keep tabs on-- pun intended.

[00:35:56.99] [MUSIC PLAYING]

[00:36:00.31] Thanks for listening to this episode of Which Investigates. If you're enjoying this season, I would love to hear which bits you found most enlightening-- or indeed, most concerning. If you're on social media, come say, hi. I'm at Greg Foot, and Which are at Which UK. We've also got the email address that you can use now too, of course. That's podcasts@which.co.uk. Podcasts with an S. And if you're really up for doing us a favour, if you've got a few spare minutes at any point, we'd love it if you can complete the short questionnaire over at Which.co.uk/investigates.

[00:36:30.52] Today's episode was presented by me, Greg Foot, written and produced by me and Rob Lilly. Editing and original music is by Eric Bria. And our executive producer is Angus Farquhar. Special thanks go to Richard Headland, Paul Lester, Kate Bevan, Andy Locklin, and Oliver [INAUDIBLE]. And I'll be back soon with our next investigation.

[00:36:48.73] [MUSIC PLAYING]