Man discovers his parents' coffee machine used 1TB of data in 10 days (dexerto.com)

660 points by ck2 18 hours ago | hide | past | favorite | 390 comments

https://x.com/NomadsGalaxy/status/2107284088247689290

help

add comment

altairprime 18 hours ago | next [–]

In the Twitter thread linked, the person confirms two things:

1. It saturated the local network with 1TB of metadata sniffing scans, *not* the network uplink to the outside world.

2. It does so because, as Keurig notes, it's collecting data about your household in order to let Keurig sell it to advertisers.

reply

khriss 10 hours ago | parent | next [–]

> as Keurig notes, it's collecting data about your household in order to let Keurig sell it to advertisers.

WTF!! When did we land in the middle of a Black Mirror episode?

I'm half convinced the first run of the LHC split the timeline and we've landed in the evil one.

reply

samsari 0 minutes ago | root | parent | next [–]

> I'm half convinced the first run of the LHC split the timeline and we've landed in the evil one.

Sadly the real answer is much less dramatic: we did this entirely to ourselves, voluntarily, purely out of lazily taking the path of least resistance offered us by companies that don't have our best interests in mind.

reply

fcarraldo 9 hours ago | root | parent | prev | next [–]

> WTF!! When did we land in the middle of a Black Mirror episode?

At least a decade ago! The first TVs with Automatic Content Recognition shipped in 2013[0]. There was also a brief panic in 2024 about air fryers spying on people[1].

And of course practically every website you visit is doing a full session recording with mouse movements and key presses captured.

[0] https://en.wikipedia.org/wiki/Automatic_content_recognition

[1] https://www.theguardian.com/technology/2024/nov/05/air-fryer...

reply

consp 4 hours ago | root | parent | next [–]

See the site this post is about. Only ~1700 trackers, and only an accept all button. Likely at least one is doing this.

reply

godelski 7 hours ago | root | parent | prev | next [–]

Ah the good old days when "we kill people based on metadata"[0] was the conversation and we thought it wouldn't get more invasive. Now we just straight up extract data

[0] https://m.youtube.com/watch?v=tL8_caB35Pg

reply

lifestyleguru 30 minutes ago | root | parent | next [–]

...and that was before 2014... over 12 years ago... now people paste into chatbot every content and any content then scan their faces, fingerprints, and documents as a routine.

reply

dahart 3 hours ago | root | parent | prev | next [–]

> And of course practically every website you visit is doing a full session recording with mouse movements and key presses captured.

Well yeah at the very least, that's Google Analytics and/or similar alternatives.

Most individual websites outside of Google/Facebook/Amazon don't get any data other than what you do on their website, so it doesn't seem quite as creepy to me as a device on your home network port scanning and sniffing other traffic.

Google and Facebook can and do 'spy' a lot, of course, but otherwise the browser does protect you from most trivial spying by random sites. Not that that's reason to feel any safer; the few people actually spying on what you do everywhere on the web are the ones with the most resources. This is all going to get way weirder with AI logs, I'm guessing.

reply

convict 1 hour ago | root | parent | next [–]

You can check this claim for yourself by opening NetworkTools in your browser, then moving your mouse and pressing a few keys to see what data is sent to the server.

reply

wcfields 6 hours ago | root | parent | prev | next [–]

I'll keep repeating this but I used to be a technical project manager for "advance analytics" for a major media agency and we used this data in our reporting for ad reach effectiveness.

I worked at a major media buyer agency "big 5" in advanced analytics; we were a team of 5-10 data scientists. We got a firehose on behalf of our client, a major movie studio, of search of their titles by zip code from "G".

On top of that we had clean roomed audience data from "F" of viewers of the ads/trailers who also viewed ads on their set top boxes. Basically any internet connected device you get is probably doing whatever it can to sniff mac addresses of your network at the least.

From a previous comment of mine:

> … my Insignia TV (best buy store brand) with fire tv built in is basically unusable. Echoing a previous comment I made too, about "smart tvs" and the "streaming sticks": Hey, have you ever thought of why even the $149 Black Friday loss-leader no-name-brand TVs all have Amazon Fire, Roku, or are now "Smart" in some way? Certainly isn't because they need to incentivise you to connect it to the internet so it acts as a Nielsen-esq measurement device of all media you view on the screen via digital fingerprints that exist in all commercial media and advertisements. [1][2]

[1] https://www.ispot.tv/

[2] https://www.samba.tv/

reply

creato 6 hours ago | root | parent | next [–]

> We got a firehose on behalf of our client, a major movie studio, of search of their titles by zip code from "G".

Doesn't Google basically make this kind of data public? I know I've seen maps by state of what people are searching for, this is barely different.

Point being, it seems absurd to compare this to snooping on people's private networks by third parties

reply

chaostheory 4 hours ago | root | parent | prev | next [–]

Let's not forget about the apps and devices that ask for Bluetooth access when it's not initially obvious why

reply

conductr 1 hour ago | root | parent | next [–]

I despise the ones that then, after you decline, tell you the app doesn't work without Bluetooth enabled although the functionality does not need Bluetooth for anything

reply

etatoby 10 hours ago | root | parent | prev | next [–]

Do you remember how a series of crazy coincidences and freak accidents kept preventing the LHC from being turned on? What if the LHC was causing world-ending or life-ending events, and we simply kept surviving only in thinner and thinner slices of amplitude (timelines) where those freak accidents happened, but where also more improbable world conditions took place?

reply

rustcleaner 5 hours ago | root | parent | next [–]

LHC is a pea shooter compared to the absolute ion cannons that are cosmic rays hitting the upper atmosphere, which are pea shooters compared to acretion disk collisions or particle collisions about a magnetar. Sorry to ruin the fun! :^)

reply

gblargg 4 hours ago | root | parent | next [–]

Recreational beliefs are fun if you don't subject them to too much scrutiny.

reply

Melatonic 7 hours ago | root | parent | prev | next [–]

Or we're in the timeline that survives because we maintain the LHC the best and it's needed for some crazy future experiment

reply

drybjed 55 minutes ago | root | parent | next [–]

Somewhere, a guy in a lab coat and with a microwave starts to laugh like a maniac.

reply

FridgeSeal 10 hours ago | root | parent | prev | next [–]

There's an SCP story like that.

World only survives, in realities where this particular creature in containment is alive. I'll see if I can dig it up.

reply

andersonpico 7 hours ago | root | parent | next [–]

SCP-7000: The Loser https://scp-wiki.wikidot.com/scp-7000

reply

irirririr 1 hour ago | root | parent | next [–]

> Item: Sudden and wholesale collapse of all extant cryptocurrency markets.

> Reactive Action: None taken; event fully consistent with long-term probability models.

heh. love scp humor.

reply

emmelaich 6 hours ago | root | parent | prev | next [–]

It was sophons.

reply

swader999 8 hours ago | root | parent | prev | next [–]

You would see my YouTube feed. I watched a couple of those and now I'm fully convinced.

reply

devmor 7 hours ago | root | parent | prev | next [–]

Sounds a bit like a doomed version of Quantum Immortality

https://en.wikipedia.org/wiki/Quantum_suicide_and_immortalit...

reply

kelipso 4 hours ago | root | parent | next [–]

Reminded me of this short story. You can only experience a life in which you are alive..

https://reactormag.com/divided-by-infinity/

reply

lwhi 1 hour ago | root | parent | next [–]

This is a great idea. We'd slowly but surely end up in hell via a process pf reduced selection.

reply

devmor 1 hour ago | root | parent | prev | next [–]

What an incredible read. Thank you for bringing this into my life - I think it's going to be one that sticks with me.

reply

sharperguy 32 minutes ago | root | parent | prev | next [–]

We were living in a "simulated" reality, where tech corporations produced amazing things a ran services practically for free asking very little in return, because it was all being funded by "stimulus" money - effectively the country getting into debt and creating money out of thin air. Once we reached the limit of this we had to face the reality of these companies actually having to pay their own way.

reply

oooyay 10 hours ago | root | parent | prev | next [–]

There is a singular patent owned by Sony that stands between you and being required to physically acknowledge ads on your TV: https://patents.google.com/patent/US8246454B2/en

reply

eru 5 hours ago | root | parent | next [–]

The patent exists, but that doesn't mean it stands between anything.

People can work around patents, or pay for licensing them etc, if they really want to do something.

reply

OneDeuxTriSeiGo 9 hours ago | root | parent | prev | next [–]

ah yes the infamous "please drink a verification can" patent.

reply

VariousPrograms 10 hours ago | root | parent | prev | next [–]

No one cares. There's little serious pushback to privacy invasions by big tech. Flock cameras have been a rare exception. Half the people "have nothing to hide" and half aren't willing to give up the convenience that the popular app or gadget gives them.

reply

n0dose 7 hours ago | root | parent | next [–]

Flock messed up courting local police departments, made it feel too real to people.

reply

DANmode 58 minutes ago | root | parent | next [–]

They will feel like they're doing great as long as they're getting paid and the cameras are up in more places than they're not.

reply

newswasboring 9 hours ago | root | parent | prev | next [–]

I'm convinced this is the state because people don't know the implications and scale of the privacy invasion. The flock camera incident shows that when people can sense, understand and feel the impact they don't like it. If we pose it as they are selling network data, nobody minds, if we pose it as they are selling your identity on the internet people get uncomfortable. But its hard to convince people of the latter. Mostly because nothing big happens due to big data breaches as someone on HN was remarking recently. Additionally, I think people have resigned to the status quo as they think that is the only way they can get their gadgets for cheap. That is just not true, companies can still make a profit without being predatory. Its just that it will not be the maximum profit.

reply

cogman10 6 hours ago | root | parent | next [–]

Part of the problem is most people don't have an idea of what's being collected.

With just a little bit of interaction with the modern internet, the profiles created are stunningly accurate. Age, gender, political ideology, favorite food, relationship status, how many kids you have.

All this stuff gets slowly collected, aggregated and shared amongst data brokers.

People would care so much more if they knew just how invasive advertising actually is. All to try and convince you to drink one more coke or grab one more cheeseburger.

reply

bushbaba 6 hours ago | root | parent | next [–]

You can't realistically stop this. The industry is international and any interaction being shared across companies allows you to build this profile. It's impossible to be fully private while having the openness of our internet interactions. You can try to limit the implications but that's it

reply

lwhi 1 hour ago | root | parent | prev | next [–]

Is my dishwasher my friend?

Maybe I should be port scanning it to make sure?

reply

pmichaud 5 hours ago | root | parent | prev | next [–]

The cruel irony of this panopticon is that I don't even get good ads!

reply

scruple 1 hour ago | root | parent | next [–]

You don't need a new toilet seat? But you just looked at toilet seats and then bought one. Are you sure you don't need another? Don't you like toilet seats?

reply

lovich 2 hours ago | root | parent | prev | next [–]

I hope it's a sign that I've poisoned my online data well enough that I frequently get ads in a language I can't speak or understand

reply

pennomi 4 hours ago | root | parent | prev | next [–]

It's going to take a modern war between superpowers to convince nations that appliances shouldn't be a ubiquitous security vulnerability.

reply

harrouet 22 minutes ago | root | parent | prev | next [–]

It started when people laughed at the EU's efforts for privacy, such as the cookie regulation or GDPR.

The first thing that Meta did after Brexit was moving its UK's user data to the US.

reply

baxtr 15 minutes ago | root | parent | prev | next [–]

Yes burn down LHC!!!

reply

3RTB297 3 hours ago | root | parent | prev | next [–]

Seriously? Literally every appliance that demands an internet connection and use of an app does this. That's why the cheapest products on the market are designed to need apps and connectivity, the prices are subsidized by the assumption of ad data to sell. Been like this for years.

Lovey example: https://frescocooks.com/platform/marketing-and-engagement

Air Fryers selling data: https://abc7news.com/post/certain-air-fryers-app-connected-a...

Student in NZ protesting it: https://www.consumer.org.nz/consumer-rights-and-campaigns/da...

Hope your TV isn't connected to the internet: https://www.cnet.com/tech/home-entertainment/tv-spying-yes-h...

reply

rebolek 5 hours ago | root | parent | prev | next [–]

LHC has nothing to do with it but American masochism can explain a lot of it. If you vote for oppressors what would you expect than oppression?

reply

podocarp 5 hours ago | root | parent | next [–]

Even if you don't vote the oppressors still come online. It's choosing between cow shit and horse shit.

reply

dofm 7 hours ago | root | parent | prev | next [–]

No, we're in a collapsing time bubble caused by an accident involving that weasel that crawled into the LHC.

April 29, 2016. It explains so much.

reply

akssri 4 hours ago | root | parent | prev | next [–]

Wait till you find out what your "Smart TV" does.

reply

dboreham 5 hours ago | root | parent | prev | next [–]

The Hitchikers' Guide to the Galaxy had the "agreement to cease to exist".

reply

aintnoprophet 10 hours ago | root | parent | prev | next [–]

Unauthorized Bread

reply

Grombobulous 18 hours ago | parent | prev | next [–]

I don't dispute the purpose of the data collection, but I can't believe this quantity of data collection is intentional.

There's no way Keurig is has the intention of paying the kind of costs required to collect a terabyte of data every two weeks for millions of people who own their coffee makers.

There must be some kind of bug here. I imagine if you unplugged it and plugged it in again the data usage would settle down.

reply

didgetmaster 12 hours ago | root | parent | next [–]

As article says, the coffee machine didn't 'collect' or phone home a TB of data. It just saturated the local network looking for data to collect. This doesn't cost Keurig or any other IoT device company a single cent. It might have been a bug, or maybe not. Without some bad press, like this post; they have no incentive to change anything

reply

MBCook 11 hours ago | root | parent | next [–]

Yeah but that can't even be useful can it? What's that going to find that *only* using 500 MB of probes wouldn't have found?

Still seems buggy.

reply

didgetmaster 11 hours ago | root | parent | next [–]

Engineer: How often should our software scan the local network looking for new devices? Once a day? Once an hour?

Manager: We might miss something. Since scanning doesn't cost us anything, better do it a thousand times a second!

reply

gerdesj 10 hours ago | root | parent | next [–]

Oh let's be charitable! A parameter measured in ms is mistakenly thought be measured in s. Hilarity ensues.

Real world example: þe Windows registry DWORD time periods seems to invite 10^-3s granularity for totally inappropriate timescales. Perhaps its considered a "best practice" by the dick heads that decide to do these things, who knows? Why bother considering how a sysadmin might actually want to use the knobs and dials and what is an appropriate value for a parameter.

I could probably find a better example but this is recent: Smoothwall has an agent (IDEX) that you install on a Windows domain controller and one of its functions can be to harvest DHCP data and pass it onto the firewall so that it can track sessions. The upload period is a registry DWORD value.

I fixed a "problem" by stopping IDEX trying to upload data a thousand times per second. I will also point out that switching on this functionality and the periodicity setting is only applied by editing the registry - there is no GUI for this. The dReal world example -ocs are clear that you should initially set 1000 as the period.

For me that sort of thing comes under the heading of "you are holding it wrong", potential victim shaming and rubbish engineering.

reply

MBCook 8 hours ago | root | parent | next [–]

This is what I suspect. A retry every X milliseconds actually being used against a variable nanoseconds, a broken loop condition that ends up always retrying, something like that.

reply

frogulis 8 hours ago | root | parent | prev | next [–]

Not really relevant, but I have to ask: why did you only use letter þ once in your comment?

reply

eloisius 2 hours ago | root | parent | next [–]

Not making an accusation, but it reminds me of a chat transcript oddity I saw while using opencode back in August. It replace a syllable of a word with a punctuation mark that has the same pronunciation or HTML entity. It was something like "...the &litude of that waveform..." but I can't remember exactly, nor which model I was using. I just noticed it and thought, that's weird. A few days later I read about text watermarking and figured it may be that.

reply

Scoundreller 1 hour ago | root | parent | next [–]

ChatGPT sometimes spit out some characters from very foreign character sets. Maybe only an issue on the free side?

reply

nom 7 hours ago | root | parent | prev | next [–]

I wondered about that too, i think they use a compose key and accidentally pressed it

reply

cobbzilla 4 hours ago | root | parent | prev | next [–]

a thorny question to be sure

reply

FabHK 4 hours ago | root | parent | next [–]

þorny?

reply

pixl97 7 hours ago | root | parent | prev | next [–]

It's impossible to tell the difference between being malicious and being ignorant.

With this particular company, everything else they do is malicious so I won't ever give them the benefit of the doubt.

I tried to use a reusable pod in one of their machines the other day and when I shut it the handle broke off leaving me rather confused. Turns out in the closing head of the machine they stuck in 4 big metal spikes to destroy anything put in there. There is absolutely no reason to do this, none, other than being dicks. Had to get out the epoxy and repair the handle of a friends machine.

So yea, screw them.

reply

johannes1234321 6 hours ago | root | parent | next [–]

The scanning is malicious.

The frequency etc. leading to 1TB is probably ignorance, but that doesn't matter as it is consequence of malicious scanning either way.

reply

mrweasel 23 minutes ago | root | parent | next [–]

The funny part is that the manufactures shitty QA made this a much bigger thing that it could have been. Had the machine done a scan once every week, which is more than enough for their purpose, diffed the result locally and pushed the few kB of data to the internet, then no one would have noticed anything.

Yes, it's malicious and completely unnecessary, but incompetence has potentially made it a PR problem.

reply

MBCook 5 hours ago | root | parent | prev | next [–]

Exactly. The whole thing is weird and creepy and wrong.

I understand why a TV would keep track of what I'm watching so they can sell the data. I think it should be illegal. It's horrible. My TV isn't connected. But the reason they would do it fits in my brain. I can see how they got there.

How a coffee machine got to running network probes… nothing. It seems like some sort of Internet of Things DEFCON presentation topic made up by putting random words together.

So to think that on top of that they were purposefully causing so much traffic on the local network is just a few steps too far for me to think *that part* was intentional.

reply

fragmede 5 hours ago | root | parent | next [–]

The reason is the same though. Probe the shit out of your network and gather data so they can sell it.

reply

mahboi 7 hours ago | root | parent | prev | next [–]

It's malicious either way. Question is whether 1TB was intended operation. I don't think it was.

reply

al_borland 5 hours ago | root | parent | prev | next [–]

I was talking to the guy who used to run our ITSM system at work. He said a team was trying to query the system 10x per second to check for updates, which was causing performance issues. Assuming it was a bug, he went to the team to have them tone it down. He was shocked when they fought with him over it. It was working as designed and they didn't want to check less frequently, despite there being no logical reason to do this.

This may be working exactly as designed, as it costs them effectively nothing to constantly scan.

reply

Refreeze5224 11 hours ago | root | parent | prev | next [–]

I don't understand giving the benefit of the doubt to a company that is actively spying on its customers, which in some jurisdictions would be illegal.

reply

MBCook 10 hours ago | root | parent | next [–]

I’m not defending the spying.

The traffic volume just sounds like a bug to me.

reply

BLKNSLVR 10 hours ago | root | parent | next [–]

A software bug in a coffee machine sounds like a problem of management not understanding the product market they're in.

reply

nekusar 9 hours ago | root | parent | next [–]

No, Management completely understands.

Closed source software/hardware is a data exfiltration device first, and the thing they're sold for secondarily.

TVs, Blurays, set top boxes, MS Windows.. All of them are the same.

reply

BLKNSLVR 9 hours ago | root | parent | next [–]

All these companies make their money as 'feeders' to the advertising industry, they just sell a different device to consumers in order to achieve it.

Selling devices to consumers is a solved problem. The problem we're currently trying optimise solutions for is selling consumers to the advertising companies.

reply

lovich 2 hours ago | root | parent | prev | next [–]

When the cost of the action to you is 0, why not do it as fast and as frequently as possible until you get your intended benefit.

Even the act of engineering rate limiting costs you more than just having this run wild over your customers networks because the vast majority of people buying these machines do not have the inclination or skills to detect this activity.

reply

sixothree 9 hours ago | root | parent | prev | next [–]

Maybe they literally just don't care about how much traffic they put on your network. Maybe the thought is "1 tb of traffic internally is very low utilization of the network over the course of a month".

reply

mahboi 9 hours ago | root | parent | next [–]

Whatever they're trying to accomplish with these scans would probably be impeded in some way by this much volume. Like it'd compete with the link it's using to phone home or overload whatever on-device processing it does with that data. The man in the article who discovered this called it a bug, I agree with him.

reply

sixothree 7 hours ago | root | parent | next [–]

"With enough incompetence, the only interpretation is malice." - SixOThree

reply

nkrisc 9 hours ago | root | parent | prev | next [–]

It uses energy paid for by the homeowner.

reply

didgetmaster 8 hours ago | root | parent | next [–]

Has anyone done the math to determine how much electricity it takes to send 1 TB of data around your local network?

reply

blackoil 11 hours ago | root | parent | prev | next [–]

Than What is the meaning of "used"?

reply

weaksauce 8 hours ago | root | parent | next [–]

local area network traffic was sent out and received by the device to the tune of 1TB of traffic. not internet data but local area network data which is not ideal for a coffee machine either way you slice it. if it were some kind of local bonjour or whatever the open standard is called service that was just alerting the network of their name it would be understandable but the coffee maker is streaming the equivalent of about 17 high def movies every day to the local network.

reply

awesome_dude 11 hours ago | root | parent | prev | next [–]

I mean, it wasn't clear to me without the explanation (I too thought it used 1TB of public internet data), but it's clear now that it is accurate (it literally used 1 TB of private network data)

It might not seem to be anything (people will assume private network traffic is free) but there is a cost - it's capacity that could be used for other purposes, eg. home alarms.

reply

b112 11 hours ago | root | parent | prev | next [–]

They could be sued in small claims court.

Here that means no lawyers, no discovery, $100 to file in plain language, and a company employee (not a company lawyer, or a contractor, or a temp employee) must attend or they default.

$15k damages.

Reasons it could happen? Imagine grandpa has a tech come out 4 times, because his network is super slow. EG, this thing pounding his wifi for its scans.

reply

zdragnar 9 hours ago | root | parent | next [–]

Small claims court in the US typically requires actual damages, and doesn't add punitive damages.

Grandpa gets reimbursed for the four techs who came out, that's it.

reply

b112 9 hours ago | root | parent | next [–]

Of course, that's the whole point.

Grandpa gets his money back. The company? Well, it has to spend money talking to a lawyer, because even though a lawyer can't attend small-claims court, they still consult.

They also have to send an employee to small-claims court, just have to deal with it. In the end it costs the company thousands of dollars maybe even over ten grand. It costs you a hundred bucks and you get your money back. That sort of asymmetry is beautiful, and if everybody availed themselves in small claims court, it would be far better than any class action lawsuit.

reply

zdragnar 6 hours ago | root | parent | next [–]

> $15k damages.

Grandpa is definitely not getting $15k in damages, and Keurig can deal with this with their in house lawyer that they're already paying a salary for. They're definitely not shelling out big bucks here. It'd be cheaper for them to let the default judgement happen than to actually show up.

reply

3-cheese-sundae 1 hour ago | root | parent | next [–]

Like everything else in today’s world: scale makes all the difference.

Let everyone file that claim for a single geek squad visit.

reply

b112 56 minutes ago | root | parent | prev | next [–]

In which case, your grandpa gets his money back, plus filing costs, plus serving costs, and if it's a default judgement, no one to argue against the gas costs, and time costs you tack on.

Please show me how this is suboptimal? Especially with LLMs to write the demand letter, and walk you through the process.

And 'using their in house lawyer' still has time cost, as does dealing with the routing and pondering the service letter. And accounting paying up. There is no aspect of your 'worst case' where it's bad. It's still all pluses. And if as I suggest, lots and lots of people do it, then they end up with a loss on that product.

If each case is $1000, or even $500 payout, how much profit does that take? Profit on 100 units? 50? If a product is horrifically bad, and everyone runs to small claims court, that's disaster for a company.

reply

mindslight 18 hours ago | root | parent | prev | next [–]

Probes create much more traffic locally than it takes to backhaul a summary of their results.

reply

sgillen 18 hours ago | root | parent | next [–]

1TB still smells like a bug

reply

nomel 11 hours ago | root | parent | next [–]

My naive assumption would be it's looking for events in time, like sign of occupancy. For example, when your phone leaves the wifi network.

But still must be a bug.

reply

Melatonic 7 hours ago | root | parent | prev | next [–]

Yeah that seems insane for text logs or any network sniffing

What kind of processor does this thing have ?

reply

mindslight 16 hours ago | root | parent | prev | next [–]

I was thinking that repeated small probes add up quicker than you'd expect. But this is ~1.1MB/sec, which still seems a few orders of magnitude off.

Now I'm left wondering what this traffic actually is - assuming probe (arp/icmp) packet size of 64 byte, that's 17kpps. I don't think an ESP32 class Internet-of-Trash chip can even do that. Even bulk transfers rather than small probes would be pushing it.

Perhaps this thing found some fellow-traveler device streaming video on a port it happened to connected to?

... the linked xit says it "broadcast 1TB of data". So maybe some protocol with a much larger packet than icmp, spammed in a hard loop without any delay?

reply

protocolture 6 hours ago | root | parent | prev | next [–]

Its just like, 1TB of LLDP/Pings/Probes/Whatever

Looks like nmap OS detection can use ~90kb per host per attempt.

reply

jimt1234 11 hours ago | root | parent | prev | next [–]

One thing that confuses me is, well, at this point in the data collection game, is there still value in this 'local' data? I mean, everyone is doing it, collecting the same data - hasn't that decreased the value? Obviously not, but I still wonder.

reply

josephg 10 hours ago | root | parent | next [–]

> everyone is doing it

Not in my house. What is even the point of connecting a coffee machine or a washing machine to the internet? I think my washing machine advertised that I could download new washing cycle programs in the app. Who on earth cares?

reply

Aerroon 8 hours ago | root | parent | next [–]

I could see its use - you could remotely activate them. Or activate them on a timer that isn't constrained by the functions of the coffee machine.

None of these are worth the spying that these companies do though.

reply

autoexec 11 hours ago | root | parent | prev | next [–]

If there's one thing you can be absolutely certain of it's that every scrap of the data they collect is either making companies money hand over fist or they strongly believe that it will soon. No company is going to bother collecting, storing, (hopefully securing), backing up, and analyzing all this data without a reason, and to them money and power are the only reasons that matter.

Right now companies are somewhat limited in how much use they can get out their horde of private and personal information, but AI is changing that rapidly. As long as you don't mind a huge rate of error (and companies don't because it all becomes "good enough" at a large enough scale) it's basically perfect for the task of digging through endless amounts of information and spewing out bullet points.

reply

burpingtree 5 hours ago | root | parent | next [–]

Ha. I feel like you have never worked for a large company if you think they are making rational decision at all. They may “believe” this will make them money, but there is no guarantee that this isn’t just costing them money hand over fist.

reply

3-cheese-sundae 1 hour ago | root | parent | next [–]

Belief and stakeholder buy-in is all that it takes for that data to be collected, no?

reply

0cf8612b2e1e 5 hours ago | root | parent | prev | next [–]

It was revealed that Honda sold data on customers for less than a dollar a piece. It’s not big money at all, but they cannot stop themselves.

reply

MarceliusK 3 hours ago | parent | prev | next [–]

I can understand a buggy device flooding the network. What's harder to justify is why a coffee maker needs to know anything about the other devices in your house in the first place

reply

amluto 6 hours ago | parent | prev | next [–]

I think it's high time for legislatures (US, California, EU, whatever) to make this kind of thing outright illegal. No consent popups. No fine print. Just illegal.

Coffee machine scans network? Nope.

Coffee machine reports things about your network? Nope.

TV does ACR? Nope.

TV reports things it incidentally learns about your listening habits? Nope.

TV transmits any microphone data or things derived from mic data that aren't explicit user commands? Nope.

Companies who collect this data even though it's illegal want to sell it or use it for marketing or transfer it to anyone else? Nope.

Company A provides an SDK to company B that does this kind of thing and company B sells the product? A is liable, civilly and criminally, and B is *also* civilly liable to the extent that they should have and did not exercise due diligence to prevent it.

Company A, company B, and/or the end user have some contract shifting liability? Nope. The parties that the law said are liable are liable, cannot use the contract to avoid liability, cannot use the contract to recover money they have paid as a result of this liability, and cannot enforce arbitration provisions.

Anyone tries to use a contract that is considered illegal under this law? That party becomes responsible for their opposition's legal fees *even if they are ultimately found not liable for some other reason*.

Police wants to buy this data? Sure, they're welcome to buy what's legally available, except that they, like everyone else, will have a hard time getting the data because it's illegal for anyone to acquire it or sell it.

It's high time to get this done. We've got this and the recent evidence of LG doing all kinds of worse crap and it really should be possible to get some legislators on board.

reply

kittomic 1 hour ago | root | parent | next [–]

GDPR, CCPA, and such laws absolutely do treat stuff like MAC addresses and network topology as legally protected information.

reply

al_borland 5 hours ago | root | parent | prev | next [–]

I would be a single-issue voter on this. If anyone running for office is doing this, and can get it done, they are getting my vote. I'm so tired of this kind of thing being normal and accepted. It has eroded the public's trust in pretty much all of corporate America, or has at least had a hand in it.

With all the hacks going on, I can't imagine why any company would even want to collect anything if they have a business model that works without it. I would think selling coffee makers and coffee pods would easily be a business model that works without data harvesting. Companies made whole businesses out of selling coffee makers alone for decades.

reply

amluto 4 hours ago | root | parent | next [–]

Why would a company integrate bullshit SDKs into a coffee maker? Because coffee maker ACR isn’t worth anything and because there are companies that will pay *absolutely freaking crazy* amounts of money, possibly in excess of the entire sale price of the machine.

https://help.earnapp.com/hc/en-us/articles/38191916327441--W...

I think Bright Data is similar but I didn’t find their authoritative numbers. It doesn’t help that my ad blocker blocks their entire domain.

reply

komali2 6 hours ago | root | parent | prev | next [–]

Why would the individuals that comprise these legislative bodies harm their retirement plan?

reply

amluto 5 hours ago | root | parent | next [–]

My general theory is that the aggregate spent on marketing is largely a function of marketers' budgets. They'll spend it in whatever way they think is cost effective, but the *amount* spent may not vary all that strongly with as the set of available marketing technologies changes.

If marketers cannot pay Google, Meta, etc to show their ads to people whom pervasive surveillance indicates are the appropriate targets, then they will pay companies (probably still Google and Meta and very likely still *American* companies) to show ads to people selected by other means. Everyone's retirement account will be just fine.

For that matter, consider who some of the biggest offenders are right now. LG and Samsung are Korean. Sony is Japanese. (But Vizio is American and seems to be owned by Walmart.) Maybe reducing surveillance capitalism will make it harder for some of these foreign companies to extract money from the US.

There's also the national security aspect. Right now, we *expect* foreign corporations to extensively spy on us. Sure, a law would not necessarily stop foreign powers from spying on us, but at least if we banned the general practice, then foreign powers who do spy on us might get noticed.

reply

gspr 5 hours ago | root | parent | prev | next [–]

Stop spreading this idea that all politicians are corrupt. You're killing democracy, and watering down revelations of specific proven cases of corruption.

I understand your feeling of despair. Of course I do. But you don't have to make other people despair. History has shown us where we end up when enough people despair.

reply

dboreham 5 hours ago | root | parent | next [–]

In the US to a first approximation they are. That makes it hard for Americans to conceive that they might not be so elsewhere.

reply

ultrahax 9 hours ago | parent | prev | next [–]

One of the reasons that all this stuff goes in its own IOT crap VLAN in my house.

reply

SlightlyLeftPad 8 hours ago | root | parent | next [–]

Ha, they will just form a mesh network with your neighbor's TV and Kuerig and upload all its sniffed coffee preferences data that way.

reply

gspr 5 hours ago | root | parent | next [–]

Or soon I guess come with an embedded 5G module and be done with it.

This shit needs to be banned, now!

reply

thedougd 6 hours ago | root | parent | prev | next [–]

That's where they want to be. Your laptop isn't interesting. You own two thermostats, an EV charger, two Samsung TVs, an LG, etc etc. The LG is watching Netflix. That's the good stuff.

reply

gruez 6 hours ago | root | parent | next [–]

>You own two thermostats, an EV charger, two Samsung TVs, an LG, etc etc. The LG is watching Netflix. That's the good stuff.

That still doesn't make any sense. If they want to collaborate to build an advertising profile, your public IP is all you need. Otherwise if they're not collaborating, what's the plan, find 0days in random IOT devices and hack them? I might be concerned about random chinese IOT devices doing that, but not devices from western companies.

reply

cogman10 6 hours ago | root | parent | next [–]

They don't want to collaborate, they want to sell.

Data brokers are buying from multiple sources because maybe a home has a keurig but not an LG tv. Or an LG tv and not a keurig.

The plan for the likes of Keurig is "These data brokers will give us free money for data from our coffee machines? Where can we sign up!". It doesn't even matter if the money translates to $0.01 per unit sold. That's probably the most disgusting part.

reply

gruez 5 hours ago | root | parent | next [–]

>Data brokers are buying from multiple sources because maybe a home has a keurig but not an LG tv. Or an LG tv and not a keurig.

Right, but OP's premise is that putting everything on the same LAN is somehow even better for the manufacturers/data brokers/ad networks/whatever, which doesn't make any sense. The only thing that actually matters is a device with internet connection.

reply

gblargg 4 hours ago | root | parent | prev | next [–]

I recently figured out how to do a vlan and set it so IoT devices can't see each other, just access the Internet (AP isolation). It hasn't broken anything so far (Matter devices excluded).

reply

clivedup 6 hours ago | root | parent | prev | next [–]

I hadn't thought of this!

Client isolation would help, but it also breaks some devices.

Are there decent daemons that allow me to allowlist which broadcast traffic to permit?

Ideally it'd be compatible with IPv6-only clients on my LAN.

reply

kevin_nisbet 7 hours ago | root | parent | prev | next [–]

Agreed, with an ACL that blocks any device to device communication within the network.

reply

whycome 18 hours ago | parent | prev | next [–]

Why is this allowed? There’s no way to consent to a coffee machine.

reply

triceratops 12 hours ago | root | parent | next [–]

If you buy a Keurig machine you've already signalled you're a sucker. (sorry)

reply

spandrew 12 hours ago | root | parent | next [–]

This is the most Gilfoyle-coded comment of the day

reply

triceratops 11 hours ago | root | parent | next [–]

I'll take that as a compliment!

reply

zikduruqe 12 hours ago | root | parent | prev | next [–]

Laughs in Moccamaster.

reply

Freak_NL 11 hours ago | root | parent | next [–]

Tongue-in-cheek, but my Moccamaster which I bought second-hand is still doing great after 15 years. Two deep cleaning sessions in all that time and just running it with vinegar a couple of times a year seems to be all it needs.

The device is dead simple. No advanced electronics. Nothing complex that can break. Just a coffee maker fine-tuned to near perfection.

The only flaw it has is the handle for the pot. I've resorted to replacing the plastic handle with a fancy walnut one I made myself. I needed that because we tilt the pot sideways to fill the reservoir with water (because of the placement on the kitchen counter and the cabinets above), and that plastic handle is not designed for sideways stresses.

reply

thinkingQueen 11 hours ago | root | parent | next [–]

You shouldn’t fill the reservoir with the coffee pot, unless you’re really washing the pot super clean after each use. Better get a proper jug for filling the reservoir, so you’re not putting coffee residue and oils back into the clean-water system.

reply

lkjdsklf 4 hours ago | root | parent | prev | next [–]

The shower head design is a crime against humanity for the cost of that machine.

reply

m463 10 hours ago | root | parent | prev | next [–]

perfect person to sell to advertisers.

Like the people who reply to nigerian emails have already been pre-qualified by 1) ignoring the misspellings and 2) replying.

reply

Neywiny 18 hours ago | root | parent | prev | next [–]

Presumably during setup and connection to the AP it has a ToS. Doubtful they just unboxed, plugged in, and it connected to the right AP and went.

reply

egorfine 18 hours ago | root | parent | next [–]

> Doubtful they just unboxed, plugged in, and it connected to the right AP and went

Why not? iirc some of the smart TVs have been shown to find open wifi networks on their own and upload data. (I'm not sure about that though. But it's plausible and undoubtedly will be implemented some day).

reply

sroussey 11 hours ago | root | parent | next [–]

The use WiFi networks as a form of GPS, much like smartphones on first stage of geolocation

reply

gambiting 11 hours ago | root | parent | prev | next [–]

I've read this argument dozens of times on HN and on HN only - I'd love to see an example of that actually provably happening anywhere in the real world.

reply

AlexandrB 11 hours ago | root | parent | next [–]

I would love to as well. It sounds like something that's plausible but potentially a minefield of liability for the manufacturer.

I could also see some kind of partnership with ISPs to use their "public" WiFi hotspots[1]. This seems more likely since it's (probably) harder to honeypot but requires making regional deals.

[1] https://www.highspeedinternet.com/resources/is-your-router-a...

reply

criddell 12 hours ago | root | parent | prev | next [–]

Maybe they bought it used?

reply

Citizen_Lame 18 hours ago | root | parent | prev | next [–]

ToS can't trump the actual law.

reply

preg_match 18 hours ago | root | parent | next [–]

The actual law is typically so weak and spineless that the ToS doesn't need to trump it. Particularly when it comes to data security or privacy.

reply

pjmorris 11 hours ago | root | parent | prev | next [–]

It is one thing to make a law, it is another to enforce a law.

reply

advisedwang 18 hours ago | root | parent | prev | next [–]

Ok, but it can collect consent

reply

anigbrowl 12 hours ago | root | parent | prev | next [–]

LOL

Legislators are cheap to purchase

reply

nicbou 18 hours ago | root | parent | prev | next [–]

It's not allowed in the EU. Not without consent.

reply

black6 18 hours ago | root | parent | prev | next [–]

It's implied consent when you give it access to your WiFi.

Why you would give a coffee maker access to your WiFi is the real question,

reply

pfannkuchen 18 hours ago | root | parent | next [–]

So in other words, they were asking for it?

reply

K0balt 18 hours ago | root | parent | next [–]

Well, yeah sorta since the only reason appliances connect to the internet is to steal data. I mean, if you buy a connected x that normally would not be connected, it’s 99 percent there to do nefarious stuff for its real owners. It’s like having a pet lion. Sure, it’s horribly irresponsible that someone sold you a pet lion, but. Uuuh you bought at pet lion. What did you think it was going to do?

Besides, did you see how he was dressed?

reply

noduerme 11 hours ago | root | parent | next [–]

This is funny.

How do you feel about thermostats? Are some things worth it? I've had a "smart" one for the past five years, part of a new furnace install, that I've stubbornly refused to connect to my wifi. Of course this means if we forget to turn the heat down while no one's home, there's nothing to be done about it.

reply

05 10 hours ago | root | parent | next [–]

There are ways to control a device remotely without letting the device spy on you and call home - Zigbee, Matter, Esphome..

reply

thatguy0900 18 hours ago | root | parent | prev | next [–]

How does this analogy go when people buy a house kitten and it turns out they have been sold a lion cub? Most people simply do not have the tech literacy to understand that what they a are buying is actually a lion, they thought they were buying a coffeemaker with some cool features. It's difficult to blame the victim when they would need to spend hours trying to understand why the thing mapping out their local network is something that they should even care about

reply

EA-3167 11 hours ago | root | parent | next [–]

In that context the person is a fool who shouldn't be in charge of another life, because they're incapable of basic prudence.

I don't actually think that applies to coffee makers spying on people though. People shouldn't be expected to understand how computer networks or ad tech spying works in the same way that literally any child or idiot should know the difference between a lion cub and a house cat.

reply

mindslight 17 hours ago | root | parent | prev | next [–]

In the analogy, there is no such thing as a house kitten. They are all cute and cuddly lion cubs. Society needs to develop a deep awareness of this, in spite of the ocean of fraudulent advertising to the contrary. (individual-liberty-protecting regulation like the GDPR would be nice too, alas)

reply

ButlerianJihad 11 hours ago | root | parent | next [–]

You have latched on to an important idea here.

Since most appliances now contain a general-purpose computer, it would be unfair to say that a device is incapable of hacking or hosting malware, because any device with the given sensors and radios and capabilities can be essentially reprogrammed at any time.

So, if we're looking at smart TVs with cameras and microphones and Wi-Fi and Bluetooth and all the connectors, or if we're simply looking at a an ordinary network device, they all fall under the umbrella of general purpose computer, and there is no way to trust their maker, or some equally capable programmer, not to turn them malevolent in some future update.

I don't view this as an issue of terms of service or of software or of your manufacturer. I view this as an existential and fundamental problem with dropping general purpose computers into your home and behind your DMZ.

Consumer operating systems like Windows and Apple have all kinds of countermeasures against this malicious use. But without the proper introspection and without the proper safeguards, a device that looks special purpose but is in fact general purpose is far more dangerous.

reply

mindslight 10 hours ago | root | parent | next [–]

Getting technical - the way I see it, the problem arises from a combination of three things - sensors/access, Internet access, and source of software/authority.

Sensors/access is unavoidable, otherwise the device doesn't actually *do anything useful*. The point is it sets the scope for what the device is able to affect. When people say "set up a separate IoT VLAN" (that still has Internet access) this is basically what they're addressing - how a device can access other devices they may care about more.

Internet access is the catalyst that's created this whole dumpster fire - I don't care about the proprietary software on my keyboard/mouse/UPS/monitor/GPU/etc to nearly the same extent. I've got some TP-Link plugs that I control local network only. They don't get Internet access, so no updates, telemetry backhaul, etc.

The authority to update/configure/change that software is the crux. With proprietary software, there are no cuddly kittens period. Here we've got a case of a "legitimate" company choosing to be a bona fide attacker to increase their bottom line! The harm was exacerbated by a bug causing it to run amok, but even without the bug they are deliberately violating trust.

But even libre software can fall to security holes as well. Meaning you want to centralize the attack surface as much as possible, for administration's sake of keeping updated. "Internet" of things is basically the direct opposite of this - postulating many illegible fine-grained links between devices on different networks. Whereas really need more like the Home Assistant model, where peripheral devices may communicate over the network, but it's only ever over the local network. Think how ethernet is set up when used in industrial control networks (or at least how it should be set up, hehe).

reply

fwip 14 hours ago | root | parent | prev | next [–]

Instead of a deep awareness, wouldn't it be easier to simply ban selling lions?

reply

mindslight 14 hours ago | root | parent | next [–]

I think the two go hand in hand, unfortunately.

reply

dovin 11 hours ago | parent | prev | next [–]

That's obviously bad and I hate it, but how much value even is there is the data that a spyware coffee machine could collect about your home? What advertisers would buy such data and what would they advertise to me? What is the marginal value of that data?

reply

paimapi 11 hours ago | root | parent | next [–]

You can also map a home out depending on signal strength. That gives you approximate size of home which gives you approximate income.

It can also correlate it with geolocation data. Google, for eg, sniffs all broadcasted SSIDs with their StreetView cars. If you can pick up on a SSID (or any of the MAC addresses of the other devices), you can buy the data set that includes it which further pinpoints demographics given the neighborhood AMI.

You can also build behavioral profiles patterns based on things like, for eg, if a baby monitor model is present or a robot vacuum, if certain devices only connect at certain times, etc.

I think the general rule for adtech is that profile guesstimates just need to be around 70%+ fidelity to determine if a sale can be made.

Lastly, you can also just sell the data on the gray market. The more datapoints, the higher the price. Most consumer product companies do that since we have little-to-no data privacy laws and the people who seem the most aware of it also are generally very apathetic and disinterested in advocating for them.

reply

Terr_ 9 hours ago | root | parent | next [–]

Also the social-graph aspect.

For example, your aged mother's phone will get pinged within X meters of an urgent-care facility, or she'll do some web-search about "hip pain", and then all the adult children start getting ads about elderly-parent-care.

Or perhaps the pervy-panopticon decides some phone-on-wifi events look like adultery, and both suppposed spouses start getting ads for divorce lawyers, private investigators, or track-covering products. (Bonus if certain specialized "adult" toys are detected on Wifi or Bluetooth...)

reply

paimapi 7 hours ago | root | parent | next [–]

Target was outing teen pregnancies back in the 2010s - https://pubadmin.institute/psychology-and-media/target-predi...

it's probably even more dystopian now with phone apps vacuuming up every last dreg.

reply

crummy 6 hours ago | root | parent | next [–]

Apparently there's some skepticism about the Target pregnancy story. https://medium.com/@colin.fraser/target-didnt-figure-out-a-t...

reply

dovin 10 hours ago | root | parent | prev | next [–]

Yeah, it definitely makes sense to me if what adtech is often doing is just backing out from specific data to a general profile like income, location, etc, so that that level of targeting can work.

reply

tomrod 10 hours ago | root | parent | prev | next [–]

Its just sick.

reply

danielheath 11 hours ago | root | parent | prev | next [–]

Knowing what TV you own, what phone models are used in your house, and what other devices you own tells advertisers about your spending patterns and income.

reply

swerve3815 11 hours ago | root | parent | next [–]

I wonder if you can identify the age of devices based just on network scans? Like if an advertiser can tell I've got a washing machine model that was last sold 7 years ago, it's time to spam me with washing machine ads.

reply

bityard 10 hours ago | root | parent | next [–]

Quite probably. nmap does (or certainly used to) have options to report the OS of a given machine had based on various quirks of the packets it got back from them. It was disturbingly accurate at times. You put that together with banner messages from running services, MAC addresses, responses to broadcast packets, deliberate probing, and the number of devices you _can't_ remotely identify on a network without actually logging into them is probably very small.

reply

dolmen 6 hours ago | root | parent | prev | next [–]

If the washing machine is on the network, its manufacturer is already aware about its age.

reply

wiml 6 hours ago | root | parent | next [–]

Its manufacturer's competitor isn't, though, and they're probably really interested in that marketing info.

reply

jz391 8 hours ago | root | parent | prev | next [–]

If you are living in a flat, this could of course be your neighbour's washing machine/TV etc...

reply

hansvm 10 hours ago | root | parent | prev | next [–]

It's a lot easier to create an embedding with equivalent information than to reliably identify a particular device, and that embedding is more than sufficient to enable targeting.

reply

ambicapter 11 hours ago | root | parent | prev | next [–]

And can be used to cross-correlate with other datasets to further narrow down who you are and how you can be targetted.

reply

NichoPaolucci 10 hours ago | root | parent | next [–]

I love that a poor, stupid man like me is being targeted by teams of the smartest data analytics professionals on the planet.

Makes me think of DraftKings. You take your average 20 something sports fan - drinking beer, watching the game. And, on the other end of that smartphone display exist some of the most complex algorithms ever designed by teams of mathematics / statistics PhDs and it's deliberately built around targeting... this one guy from Florida who is pretty sure his team will be up by 7 at halftime.

Maybe it's more of a morbid joke, but it makes me laugh to think about.

reply

BLKNSLVR 10 hours ago | root | parent | next [–]

The way you explain it really captures how predatory the behavior is.

It's an accurate explanation.

reply

tomrod 10 hours ago | root | parent | prev | next [–]

My income is low. Ignore me, advertisers, you have no power here.

reply

hansvm 10 hours ago | root | parent | prev | next [–]

They can get a profile of when you're in which room, how many people are in the house, etc. That's useful for targeting (e.g., up at 5am, leaves, comes back in an hour or two will have you profiled (more complicated than this since it's usually a fuzzy vector thing, but for the sake of argument) as somebody who goes to the gym, maybe leading to creatine advertising or other whatever), and also for attribution (e.g., a TV ad is shown, somebody gets up, and a purchase is made from a device known to exist at that household, regardless of whether it's behind a VPN).

If you have even very crude data from somewhere else for the targeting, improvements in attribution tech are actually the more important factor. The adtech company mostly doesn't even care who you are, just whether the ad turned into a purchase or not, and that's where a lot of the invasive tracking comes from. They'd be perfectly happy with a quickly changing "identity" if they knew it was reliable and stable between ad and purchase.

reply

Quinner 11 hours ago | root | parent | prev | next [–]

If it scans the network and sees a smart dishwasher, smart washer/drier, and smart lights, but no smart fridge, I imagine its worth something to a company like Samsung to start targeting that customer with ads for a smart fridge.

reply

srcreigh 10 hours ago | root | parent | prev | next [–]

It’s not so hard to get root shell on some routers via the admin panel, which usually has the same password as the wifi network or a default password. From there the device can capture dns logs.

reply

jacquesm 10 hours ago | root | parent | next [–]

That would be a crime, wouldn't it?

reply

ted_dunning 9 hours ago | root | parent | next [–]

Depends on the click-through license that linked to the terms of service that you agreed to as part of buying the machine.

reply

reaperducer 9 hours ago | root | parent | prev | next [–]

It's in the Terms of Service you agreed to when you looked at the box it came in at the store.

reply

eckelhesten 11 hours ago | root | parent | prev | next [–]

All data is valuable. Even something as simple as the MAC address to your iPhones WiFi or Bluetooth chip is worth something to dataprofilers.

reply

dovin 10 hours ago | root | parent | next [–]

This does seem to be true in the age of throwing all data in to training the next iteration of the God Machine, but also, some data is a lot more valuable than other data and I want to know what the incentives are of people who are collecting data in our homes and what the actual data / derived data that they're after.

reply

r_lee 6 hours ago | root | parent | next [–]

big thing is to be able to serve ads more effectively

so if you know that a user is having an affair, you might want to serve divorce lawyer ads (I'd imagine those are very expensive) or something.

this kind of data though is just like a cog in the machine, but it can e.g. give enough info to know how many people likely are in that household, and so on. useful when combined with other signals

reply

adamrezich 9 hours ago | root | parent | prev | next [–]

That new Amazon page that shows you what it has inferred about you told my friend that he “clips [his] fingernails approximately every two months.” He makes extensive and enthusiastic use of Echo products in his household, but I have no idea how it could've possibly reached that conclusion (and neither does he!).

reply

scun 6 hours ago | root | parent | next [–]

The spookiest thing about the Nail Clipping Song is that you immediately forget singing it, or even knowing it.

reply

lenkite 10 hours ago | root | parent | prev | next [–]

> but how much value even is there is the data that a spyware coffee machine could collect about your home? What is the marginal value of that data?

Scale it up - make that millions of homes. Now there is godlike strategic value. Esp when "borrowed" by 3 letter agencies.

reply

dovin 10 hours ago | root | parent | next [–]

Yeah, that seems like the kind of dataset they would like to keep in their back pockets

reply

jimrandomh 9 hours ago | parent | prev | next [–]

It doesn't sound plausible to me that the main buyers of this information would be advertisers. It sounds more likely that the buyers are black-hat hackers, or intelligence agencies. The main reason someone would want a map of all of the devices behind your home router is so they know what to target first for exploitation, if they want access.

reply

radio879 9 hours ago | root | parent | next [–]

There are companies that sell people's home ip address as a VPN/Proxy for anyone who wants to use it for anything. They call it "residential ip's". People use them for web scraping, but probably tons of illegal stuff too. AI companies use them to not get blocked.

I've heard that they put it in IoT devices, free Android apps that people use on their TVs, free phone apps, games, prob lots more.. The companies advertise it like its super safe only legit normal people borrow the internet from these people but then in fine print it'll say its not our responsibility etc.

What I have been wondering is - since they don't seem to care or check what people are using the "residential ip's" for, what happens when someone does a bunch of illegal stuff on some random person's home IP and ends up raided by cops?

I feel like the world is going in these directions.. the excuse is always "well, they clicked Yes on the Terms of Service! They agreed to it!"

reply

h1fra 19 minutes ago | parent | prev | next [–]

We need to regulate the shit out of this kind of stuff. Flat out ban all data collection by home devices.

reply

gblargg 4 hours ago | parent | prev | next [–]

I tend to face the problem of too many choices with products. I'm actually thankful that manufacturers like Keurig are voluntarily taking themselves out of the pool of consideration. It makes my decisions easier. I can only see things getting even easier as time goes on.

reply

smt88 4 hours ago | root | parent | next [–]

Keurig makes zero high-quality products so this story shouldn't have changed much anyway

reply

Waterluvian 7 hours ago | parent | prev | next [–]

I love how I'm expecting Keurig to feign innocence but instead they're just happy to admit it.

reply

zahlman 5 hours ago | parent | prev | next [–]

How do I exhaustively check for whether devices in my household are doing this? Is it enough that I don't see them on my desktop's list of available networks?

reply

dboreham 5 hours ago | root | parent | next [–]

No. You'd need a packet sniffer. Wireshark or similar. And a layer2 setup that lets you see non broadcast traffic from the target device.

reply

dolmen 7 hours ago | parent | prev | next [–]

Could you post the Twitter link?

Because the article is also full of 238 advertisers.

reply

zahlman 5 hours ago | root | parent | next [–]

It's been added to the OP: https://x.com/NomadsGalaxy/status/2107284088247689290

reply

WheatMillington 8 hours ago | parent | prev | next [–]

What kind of idiot is connecting their coffee machine to the network?

reply

dolmen 6 hours ago | root | parent | next [–]

Schedule the morning coffee in HomeAssistant?

reply

AnimalMuppet 18 hours ago | parent | prev | next [–]

To me, this is *begging* for a class-action lawsuit.

Yeah, sure, the terms of service probably say that they can do that. That's still in "unconscionable" territory. And courts do not like unconscionable contracts. If it's unconscionable, it's invalid (if I understand the law correctly).

Is *this* why everybody wants to make appliances with wireless?

reply

criddell 12 hours ago | root | parent | next [–]

You would have to show the judge how you have been harmed and the judge will want to know what the damages are.

reply

altairprime 18 hours ago | root | parent | prev | next [–]

Yes, this is why everybody wants to make vehicles and refrigerators and thermostats and ereaders with cellular and/or wireless: subscription revenue from bulk data purchasers of what their scans reveal. IIRC Amazon was an industry leader in this space by showing book authors what page you stopped reading on, and then bulk assessing that data at scale to estimate which sentence or word; of course, Google's Android remains the most successful at-scale deployment of data collection for advertisers worldwide. See also, for recent context, the top comment (and others) of *the LG Smart TV problem* (30 days ago, 1012 comments) https://news.ycombinator.com/item?id=49592375

reply

kotaKat 18 hours ago | root | parent | prev | next [–]

Funny thing, that. Go into an electronics store now and pay attention to the TV boxes and the printer boxes. The amount of crazy fine print on both of them now is absurd. The printer boxes all now have lots of fine print about the various ink protection and DRM schemes and subscription services, the TV boxes have everything ranging from binding arbitration on the box (LG) to " (brand) accounts are REQUIRED to use this TV" (Visio).

Customers are gonna get lost in the sauce and skip right past all of that and toss the packaging.

reply

seb1204 11 hours ago | root | parent | next [–]

Enshittyfication of everything

reply

jerf 11 hours ago | root | parent | prev | next [–]

"Is *this* why everybody wants to make appliances with wireless?"

Which raises in my mind the obvious defense, which is that if you try to put four or five of these devices on your network they'll be too busy interfering with each other for them to actually spy on anything.

Let the wiretaps wiretap the wiretaps. Keeps 'em busy, makes 'em feel like they're doing something important.

```
> What is my purpose?

You wiretap the wiretaps wiretapping our wiretaps.

> Oh my god.
```

reply

mahboi 9 hours ago | parent | prev | next [–]

As in, port scanning or ARP spam or what? Twitter randomly decided I'm a bot

reply

KellyCriterion 18 hours ago | parent | prev | next [–]

Reg 2:

But why do they need to collect 1 TB? Sounds like a lot of redundant/doublicated entries then for a small network?

reply

rasz 18 hours ago | parent | prev | next [–]

> as Keurig notes, it’s collecting data about your household in order to let Keurig sell it to advertisers.

its LGs glass in LG household, and now Keurigs kitchen

reply

hn_throwaway_99 2 hours ago | parent | prev | next [–]

> It does so because, as Keurig notes, it’s collecting data about your household in order to let Keurig sell it to advertisers.

This is either outright false or at least highly misleading. Keurig says they may sell information *about your coffee brewing habits* to third parties (i.e. your usage of the coffee machine itself), but nowhere does "Keurig note" that they collect other data about your household through network scans and sell that to advertisers.

I'm not even sure which tweet you were referring to that implied that. In any case, there are tons of responses here that are interpreting your quote as saying Keurig admitted they do network scans to acquire info about your household to sell to third parties, and that (the idea that Keurig says they do this) is flat out false.

reply

isolli 3 minutes ago | root | parent | next [–]

Thanks, I came here to challenge this too. I cannot find any tweet supporting the OP's second assertion.

reply

xyst 6 hours ago | parent | prev | next [–]

Keurig Exec, probably: "We own the coffee"

The people that said LG isn’t the only company doing invasive data harvesting is sadly correct.

How did we as a society let it get to this point?

reply

lazide 18 hours ago | parent | prev | next [–]

#1 - why? #2 - oh, because fucking yikes.

reply

malbs 5 hours ago | prev | next [–]

I'm sceptical only because this is a screen shot of unifi client info, and unifi seems to have some bug that will report devices as using terabytes of data in the last 24 hours, which is obviously not true..

Here's an example from my unifi dash right now, my laptop has done 24tb of data? lol email and web browsing

https://imgur.com/a/I54vcYR

reply

doublepg23 5 hours ago | parent | next [–]

I posted the same below, they’ve had similar bugs for the ~decade I’ve used them.

reply

MarceliusK 3 hours ago | parent | prev | next [–]

This is why I'd really like to see a packet capture or at least some interface-level counters

reply

drop_the_mike 7 hours ago | prev | next [–]

I'm not the most versed with networking or operating systems but I wonder how difficult it would be to program a raspberry pi to poison the datasets of these types of things. Program it to impersonate a wide set of devices and randomly respond as such in a home. Or even if it would be worth it. Maybe if a phone app could do it too that would make it easy to poison the dataset only when you purchase new smart devices while they do their heavier reconnaissance during the first few weeks (assuming Keurig and the like calm down a bit after some period of time).

reply

judge2020 6 hours ago | parent | next [–]

The only financial impact to them would be your single ad profile. They don't care about having the widest and most accurate knowledge of all devices on their customers' networks to sell as some dataset, they want to target ads at you based on which products you have - and maybe get a bigger payout if it finds something on your network that it advertised to you a whole ago, as that confirmed conversion is worth a ton to advertisers.

reply

dannyw 3 hours ago | parent | prev | next [–]

Plug for https://adnauseam.io/ ; which is banned from the Google Web Store.

Yes, they can trivially build systems to filter this out, but your favorite coding agent can probably make it more stochastic / clever ;)

In my experience, this has basically 'neutered' personalised advertising for me (I get all kinds of ads, in all kinds of languages, when using my Google account or network w/o an adblocker); so it definitely has an effect.

reply

MarceliusK 3 hours ago | parent | prev | next [–]

My concern is that poisoning the dataset doesn't really stop the scanning. The device is still poking around your network

reply

gblargg 4 hours ago | parent | prev | next [–]

If I had a machine like this on my network, I'd be tempted to figure out where it's sending the telemetry data, and help it out by sending a LOT more. It would be funny if they blocked my IP because I was reporting too much data.

reply

IronyMan1 2 hours ago | parent | prev | next [–]

Maybe add LLM prompts to poison whatever system is analyzing the Data?

reply

sam-cop-vimes 11 hours ago | prev | next [–]

This website values your privacy. Only shares data with 1747 partners.

reply

cuu508 3 hours ago | parent | next [–]

It values your privacy in the sense that "it is absolutely worth something so I'mma take it thanks"

reply

consp 3 hours ago | parent | prev | next [–]

And nice dark patterns to not allow you to reject that.

reply

crazybonkersai 1 hour ago | root | parent | next [–]

You can. First by clicking view partners and then save and exit. Shitty ux though

reply

doublepg23 7 hours ago | prev | next [–]

Nobody has mentioned this but the tweet in question is a screenshot of a UniFi dashboard which is notorious for miscalculating bandwidth usage.

reply

bombcar 4 hours ago | parent | next [–]

Get out of here with your reasonable explanations, we're having a hissy-fit and a lynching!

reply

BLKNSLVR 10 hours ago | prev | next [–]

So, separate VLANs, wifi isolation and complete internet blocking for all devices such as this, and only purchase devices that can be controlled via Home Assistant.

What hope do normies have?

reply

denkmoon 10 hours ago | parent | next [–]

You don't need separate VLANs, wifi isolation and firewalls. You need to reconsider putting a coffee machine on the internet lol.

reply

crystaln 3 hours ago | root | parent | next [–]

Something tells me it's not just coffee machines that do this, it's lots of appliances that have useful online capabilities.

My LG washer/dryer tell me when loads are done and when someone lets wet clothes sit in the washer. This is priceless. But yeah they are probably profiling my house.

reply

fdgfikgfv 8 hours ago | root | parent | prev | next [–]

Exactly. I have bunch of appliances that are wifi enabled but they work just fine without it. The stories like these and of firmware updates bricking the appliances is enough to never really look at the benefits of connecting.

Sometimes I like the idea of preheating oven on my way home but then I get home and forget about it.

reply

mrheosuper 6 hours ago | root | parent | next [–]

Well, you could connect your oven to HA, and VPN to your home.

reply

dietr1ch 9 hours ago | root | parent | prev | next [–]

Can they? It seems that surveillance data will be able to subsidize coffee machines and make it so you get a better machine for the same price, or an equivalent, cheaper one.

reply

olelele 9 hours ago | root | parent | next [–]

Or it is the same crap just w spyware? My stainless Bialetti was invented about a hundred years ago and cost less than 50€.

reply

BLKNSLVR 8 hours ago | root | parent | prev | next [–]

Sometimes, and I don't think this is one of those examples, 'family' makes such things necessary.

reply

sfRattan 9 hours ago | parent | prev | next [–]

> What hope do normies have?

None, without people like us in their families who are able *and willing* to help.

We as computer people need to internalize and accept the idea that helping our immediate and even extended family with technology is now part of defending human freedom. *And we need to form ourselves into the best helpers we can be by learning how to teach and communicate well*.

reply

tombert 9 hours ago | root | parent | next [–]

> None, without people like us in their families who are able and willing to help.

I am able and willing to help my parents get off of a lot of the spyware bullshit they have throughout their house, but they don't want to hear it. They liked the connected stuff and I think that they think I'm a little weird when I push back about why we can't trust corporations like Google or Microsoft to do everything.

reply

ssl-3 44 minutes ago | root | parent | next [–]

I like my connected stuff, too, and I'm not a normie.

I don't *need* voice-activated lights for the basement for when I head down there with my arms full of laundry, or with a bunch of food to put into the freezer, or whatever shit I'm carrying. I don't need them to turn themselves back off after a time, either.

I mean: I could use any of a wide array of motion sensors, but they'll turn the lights on even when I'm just working in the kitchen near the basement stairs. (Or maybe I could use a beam curtain! Yeah! Now they only respond when a beam breaks, instead of when I'm working in the kitchen near the basement stairs!)

Or I could just put the shit down and flip the switch.

Or: Plan ahead, and flip the switch in advance. And then just flip it back off when I'm done down there.

On a long-enough timeline, someone will find a way to make a point of explaining that any combination of a lack of planning and a lack of effort is completely and utterly inexcusable. That every action should should be planned, and that every manual effort has value.

But I chose this path anyway, and I like it this way. I invited the spies into my home very deliberately. The basement light automations work great, by the way, and the default non-voice UI is the same, plain, old-school light switch that the house came with.

(I also chose to carry an always-on pocket supercomputer with me wherever I go even though I have no way to observe what that thing is really doing at any given time.)

reply

judge2020 6 hours ago | root | parent | prev | next [–]

"They like their connected stuff" means their barrier isn't "I don't want a corporation processing my data", it's "I want to be in charge of my interactions with it". That changes what sort of recommendations you can bring to them. An all-or-nothing mindset is rarely the correct way to change someone's mind.

Recommending they turn off ACR and other spyware on their TV is based on recent reporting is good and backed up by said reporting. Probably even recommending against too-good-to-be-true connected doorbells even.

Meanwhile, telling them not to use a first-party Google, Amazon, or Apple smart home speakers is a bit questionable when there's been pretty good audits over the years that show they really do only do wake word detection. You'll just sound like a crazy person if you can't point to some reporting on a device doing bad.

reply

sfRattan 8 hours ago | root | parent | prev | next [–]

Getting better at communicating is unfortunately really hard. And it must pair with the *helper* aspect: you've got to also provide value.

"Nomad," the guy from the article, was already administering his parents' home LAN.

How do you get there? "Mom and Dad, we're going to set up your home network so that it's blended with my home network. To all the machines in your house and mine, it'll look like they're on the same network together. That'll make it easier for me to help you with any tech problems you're having, on your computer or on any smart device. The connection between our houses will be encrypted and secure" You're installing a router/firewall for them and adding to your WireGuard overlay network, but you're not using any of those words to tell them what's going on.

What to do next? "How was watching TV last night from {$TIMESTAMP_A} to {$TIMESTAMP_B}? Yeah, my network sentinel detected that your TV was sending your viewing habits out to somewhere on the Internet and warned me and blocked it. I can't tell what you were watching, but {$TV_BRAND} sure can." You're monitoring their LAN via the router/firewall you've set up, but you are again not using technical language.

Wherever spying is invisible and frictionless, make it loud and incessant. And continue to provide value to the family on the shared overlay network. Photo and home video backups, media server (it's like Netflix!), mutual offsite buddy backups, password management, a local Minecraft server for the kids and the cousins.

Cultivate a family network garden that is good enough to consider leaving the leviathans behind and build walls around it that are high enough to commit to leaving the leviathans behind for what is now a garden inside a family network castle.

reply

BLKNSLVR 5 hours ago | root | parent | prev | next [–]

Yeah, I have some relatives that wanted me to turn off the ad blocking because it meant they couldn't watch ads on their mobile games in order to earn more lives / game time.

Folks be crazy.

reply

aksss 5 hours ago | root | parent | prev | next [–]

Heh, less like an episode of Black Mirror and more like LOTR. We hobbits have a duty and can't afford to not care about the world outside our shire.

reply

lstodd 9 hours ago | parent | prev | next [–]

Normies have a cezve.

reply

BLKNSLVR 5 hours ago | root | parent | next [–]

In that case, I don't think I've met many normies.

reply

jakub_g 10 hours ago | prev | next [–]

The real question is: could someone explain me why anyone would want a smart coffee maker?

What kind of functions it has that can't be replaced by:

- walking a few meters and pushing a physical button

- waiting a whopping minute for coffee to brew, instead of triggering it remotely

reply

looperhacks 7 minutes ago | parent | next [–]

A smart coffee maker is one of the earliest smart home appliances: https://www.rfc-editor.org/info/rfc2324/

reply

el_benhameen 8 hours ago | parent | prev | next [–]

I have an admittedly very specific set of constraints that led to me buying a wifi kettle. I:

- have a short window to get to the train in the morning - want coffee on the train - don't particularly like drip machine coffee - want the water boiling when I wake up so that I can make coffee and get out of the house as quickly as possible - am more morally opposed to waking up five minutes earlier (pushing my wake time into the 4 o'clock hour) than I am to having a smart device.

I couldn't find a kettle that runs on a timer, and just taping the switch in the "on" position and hooking it up to a plug timer felt unsafe, so getting a stupid wifi kettle and using their stupid app to set it to auto-start was the best option. It's on its own network, though.

reply

fma 7 hours ago | root | parent | next [–]

I have a smart plug that can turn on and off...I have my coffee maker switched on, and it only switches on when my wifi plug is on. So I can have the water heating before I come down stairs. Whether it's better than a smart coffee maker or not I'm not sure - but at least I have a popular device that has more eye. Not sure how many people are looking at niche coffee makers.

reply

smt88 4 hours ago | root | parent | next [–]

Smart plugs all say not to use them with appliances because the wattage is too high. You can melt one or start a fire if you're not careful.

This is possibly not an issue with a regular drip coffee machine. It's definitely an issue with a kettle or, say, air fryer.

reply

timvdalen 59 minutes ago | root | parent | next [–]

Do they? The IKEA ones are rated for 3680W, which is plenty even for an appliance on a dedicated 220V 16A circuit.

reply

mzhaase 31 minutes ago | root | parent | prev | next [–]

My understanding, and I would love for someone to explain why, is that they measure current with a shunt resistor which is fine for inductive loads like a water heater, but not fine for a big motor for example.

reply

lexicality 52 minutes ago | root | parent | prev | next [–]

IKEA's smart plugs are all rated to carry the full wattage allowed by their plug types for resistive loads (though only 300W for motor loads)

reply

catlikesshrimp 2 hours ago | root | parent | prev | next [–]

You could use the smartplug with a relay to a higher capacity non smartplug.

reply

stonedivot 3 hours ago | root | parent | prev | next [–]

These aren't constraints. These are preferences. Framing them like constraints makes it sound like the whole situation is out of your hands, and therefore owning a smart device is practically thrust upon you by external forces.

Just say it: you bought a smart kettle due to your completely adjustable preferences.

reply

ssl-3 1 hour ago | root | parent | next [–]

We are constrained by the decisions we have made based on the preferences that we maintain.

Thus-constrained, this person states that they're able to get 5 more minutes of sleep every night and still make coffee before taking the train to work. That's ~25 minutes per week, or ~1.8 hours per month.

They didn't have to choose to go to bed earlier in order to gain this time and still make coffee in the morning. They were going to make coffee with a kettle anyway and were constrained by a the necessity of maintainining ownership of a kettle with which to do that.

So they simply selected a kettle that can be safely automated so as to be ready at the right time every morning instead of one that cannot be. In exchange, they gain around 20 hours per year, for every year that this kettle lasts for. (What would you do for nearly an entire extra day, per year?)

Sure: It's adjustable, just as many constraints are.

Maybe there's even a coffee shop around the corner that they could work at instead, and they could just walk there and brew themselves a cup of coffee using the hot tap on the espresso machine before they start their shift -- and skip the train.

But maybe that wouldn't fit into the constraint of being able to support the dwelling that they prefer to live in.

So maybe they could soften that constraint as well, and live a little lower. (Maybe they can soften enough constraints that they can just live under a bridge somewhere, with no permanent dwelling, no job, and no coffee. Perhaps, if we look hard enough, we might find that even the constraint of living a life -- at all -- is also adjustable.)

reply

gfrtgfrtgfrt 8 hours ago | root | parent | prev | next [–]

so you brush when you wake up right? The brushing takes about five minutes. The kettle probably takes less time than that. Probably two minutes in my experience. Why not just wake up fill up water click it on and then brush. I mean, you could even keep the water filled up the previous night.

I do feel that over-automation is a thing

reply

el_benhameen 7 hours ago | root | parent | next [–]

I don't disagree that over-automation is a thing. I miss my more leisurely mornings!

I use a Hario Switch to make coffee. It takes 3:30 to brew, so I pour the water and then brush my teeth and prep while waiting. Async coffee! I'm out the door as soon as the coffee is in the mug and get to the train station about 2 minutes before the train arrives.

reply

noisy_boy 5 hours ago | root | parent | next [–]

The margin of error is razor thin. As tight as a global supply chain. I'm worried about your living on the edge like that.

reply

warkdarrior 4 hours ago | root | parent | next [–]

Yeah, what if Iran, Trump, or the Houthis blockade his/her route to the train station?

reply

smallnix 10 hours ago | parent | prev | next [–]

Maybe they want to save their extraction & profile curves per recipe in the cloud or something. Or for less advanced devices, simply notifications to change the filter I guess.

reply

arielcostas 9 hours ago | root | parent | next [–]

I mean, if you really want profile curves and so on, it could just save it to some sort of SD card, or if you want to be really fancy sync it via bluetooth to a mobile phone with an app. Same with the notifications to change the filter or whatever, or a damn light on the machine. Right?

reply

boplicity 9 hours ago | parent | prev | next [–]

I have a very old school manual espresso machine (a La Pavoni). It's connected to a "smart" plug, which lets me turn on the machine remotely, and have it turn on automatically in the morning. It's nice to have it heated up and ready to go when I wake up. Nothing about the machine is smart though.

reply

WheatMillington 8 hours ago | root | parent | next [–]

My Bambino takes 4 seconds to warm up from a cold start.

reply

simlevesque 10 hours ago | parent | prev | next [–]

The problem is that when I want to make coffee, I'm my most stupid self I'll be all day.

reply

361994752 9 hours ago | root | parent | next [–]

So you won't want the coffee machine over smart you at that time...

reply

Rury 7 hours ago | parent | prev | next [–]

These sorts of products aren't typically driven by consumer wants. Rather they're typically driven by B2B/sales/marketing/investor types, who are primarily focused on finding/addressing secondary markets for further profits, more so than it is about addressing core consumer wants.

In other words, these product decisions aren't really made on the rationale that internet connected coffee makers make sense from the standpoint of a consumer who simply wants coffee made...

It's more: "let's make smart coffee makers so that we can sell to 2 markets:

```
1) a coffee maker to consumers who want coffee made

2) consumers data/eyeballs to advertisers who want their info/eyes
```

... and make more profits for ourselves".

reply

WalterBright 1 hour ago | prev | next [–]

I checked Amazon's "About You" page, and it said:

```
"Performs chainsaw work"
```

I'm satisfied with my manliest man profile. Amazon nailed it.

reply

ttytty 18 hours ago | prev | next [–]

It's so important to have a dedicated VLAN (or 2.4g SSID) for IoT devices and block access to your regular VLAN/SSID or enforce some more granular rules on what devices can communicate with each other.

Most non-ancient routers/gateways support this. There are way too many IoT devices running code that's _worse_ than what older LLMs produce.

reply

Levitating 12 hours ago | parent | next [–]

This is good advice but a simpler solution is to just not buy these things? Coffee machines don't need internet. Your thermostat doesn't either.

reply

bartread 10 hours ago | root | parent | next [–]

I agree on the coffee machine. On the thermostat, not so much. We keep pretty irregular hours so being able to control the thermostat remotely, so the house isn’t being heated unnecessarily but is warm on our return, is useful.

reply

sfRattan 9 hours ago | root | parent | next [–]

Honeywell Home T6 Pro Z-Wave.

It's smart and supports only Z-Wave, not WiFi. So something like a machine running Home Assistant must sit between it and the Internet. And then its up to you to decide how you want to do remote access, but WireGuard overlay networks (e.g. Netbird, Tailscale) basically solve that problem at home-user scale.

reply

microtonal 1 hour ago | root | parent | next [–]

This. We should buy Z-Wave or Zigbee as much as possible (Matter over WiFi/Thread can access the internet, so are out) to grow that market. Both are completely disconnected from the internet and you decide how such devices can be accessed.

Reject all the WiFi-connected stuff, unless it's very user-centered and worst case you can upload your own firmware (e.g. a bunch of Shelly devices).

reply

magicalhippo 9 hours ago | root | parent | prev | next [–]

That said, getting a Zigbee or Z-Wave thermostat and have Home Assistant or similar control it is a better option that buying a surveillance-ready WiFi-enabled one.

reply

pezezin 7 hours ago | root | parent | prev | next [–]

If the house is well insulated, keeping it at a constant temperature might be more efficient than running irregular cooling/warming cycles.

Plenty of houses are not well insulated though...

reply

stronglikedan 11 hours ago | root | parent | prev | next [–]

> Coffee machines don't need internet. Your thermostat doesn't either. reply

Yours may not, but that's just your personal preference. A lot of folks enjoy these products. An argument could be made that no one needs a coffee machine or thermostat to begin with.

reply

askvictor 10 hours ago | root | parent | next [–]

I can definitely see the case for an internet connected thermostat. A coffee machine, much less so.

reply

delecti 10 hours ago | root | parent | next [–]

You're about 35 years behind the times about people networking their coffee machines [0]. People might want to know the status of the pot (the OG example), how their ground/bean coffee supply is, or the ability to trigger a coffee or water boiling before they walk to the machine. My coffee making process is entirely manual, and I like it that way, but I can at least see how there are some features that could be nice.

[0] https://en.wikipedia.org/wiki/Trojan_Room_coffee_pot

reply

randerson 11 hours ago | parent | prev | next [–]

It's not enough to simply have a IoT VLAN that you put all your IoT devices on. Because those devices can see one another. In this case, if the coffee machine can see what type of smart fridge and smart toaster you're using, they can sell that data.

I default to adding IoT devices to a 2.4g "Guest" network where they can't see each other. Exceptions are IoT devices that need to see their friends to do what I bought them for, or devices I want to integrate with HomeAssistant. In those cases I create a separate IoT device per IoT brand. Excessive but necessary.

reply

microtonal 1 hour ago | root | parent | next [–]

In those cases I create a separate IoT device per IoT brand.

That requires a lot of SSIDs though and AFAIK it reduces airtime for each SSID on the same router (which may be bad if you also use 2.4GHz for your regular devices).

So far two separate VLAN + SSID (IoT-Good and IoT-Bad) with client isolation on IoT-Bad has worked pretty well for me. In some cases mDNS advertisements have to travel at least from the IoT VLAN to the VLAN HA is on for the devices to be discovered.

reply

ssl-3 13 minutes ago | root | parent | next [–]

SSIDs are indeed expensive in airtime.

There's ways to reduce the expense like changing DTIM interval (for less-frequent broadcasts) and increasing base data rate. Few folks in 2026 have anything at home that requires the 1Mbps base rate of 1999's 802.11b anyway, and slower DTIM can have other advantages, so these tend to work well at increasing available airtime for more SSIDs.

There's an additional trick that can also be used, though: Wifi client isolation. This lets the IoT widgets share an SSID and VLAN with which to talk to the HA machine and/or their cloud-based mothership(s) or whatever, but without being able to see eachother on the SSID.

It still needs set up right lest stuff walk right by it, but it's an available feature.

A smart coffee machine may need to talk to some kind of controlling endpoint (whether local or afar) in order to do whatever it does. It does not need to be able to enjoin in a conversation with my light bulb in order to get there. But that doesn't mean that they can't share an SSID. :)

reply

pjmorris 11 hours ago | parent | prev | next [–]

My Bialetti Moka pot doesn't attempt to acquire an IP address.

reply

ErroneousBosh 10 hours ago | root | parent | next [–]

I'm in Rome right now.

There's a Bialetti shop on the road between the flat I'm staying in, and the Metro station.

If I'm not careful this is going to seriously damage my wealth.

reply

jjgreen 10 hours ago | root | parent | next [–]

They're not expensive and last a lifetime, get one.

reply

mindslight 16 hours ago | parent | prev | next [–]

Of course by VLAN, I presume you mean one that doesn't have access to the Internet.

FWIW preventing the harm that happened here would seem to require a second set of APs (radios) on a different channel.

reply

pseudohadamard 18 hours ago | parent | prev | next [–]

I have a firewall that tells me how much data each device is uploading and downloading. One particular device pulled down 6GB a week and uploaded 1.5GB doing absolutely nothing. I mean literally nothing, I use the local API to communicate with it. Blocking the one domain it was doing this to dropped traffic to essentially zero with no loss in functionality.

reply

HPsquared 17 minutes ago | prev | next [–]

Smart devices go on guest wifi

reply

andridk 1 hour ago | prev | next [–]

To me, it's unthinkable to discover this and not try to figure out what the hell that coffee maker was sending. He should donate the machine to a security researcher.

reply

altern8 11 hours ago | prev | next [–]

Can someone explain to me what kind of data it collects, and what value could that data have to advertisers or anyone else?

reply

rwz 10 hours ago | parent | next [–]

It collects the data about your home appliances and personal devices. This data can tell a lot about your income level and spending habits. This is extremely useful for advertisers for obvious reasons.

reply

altern8 10 hours ago | root | parent | next [–]

I see, like how many cell phones are in the household and what brand

reply

rwz 10 hours ago | root | parent | next [–]

Right, or laptops. Or TVs. Or other IOT devices like coffee makers, dishwashers, washers, garage openers, smart locks, vacuums etc.

reply

wcfields 6 hours ago | root | parent | next [–]

This data is used in aggregate to decypher household penetration and refine known data about demographics and household income.

Here's an example of the sorta-end-game: Currently they can know how many kind of "devices" are in your household and using probabilistic statistics give a decent n value of how many "devices" are in a certain zip code. Using that, your advertising can become more efficient by only buying ads in zip codes that contain certain "devices".

I say Zip code because that's what I've worked on in the past at the most granular level for Marketing Mix Modeling or MMM. You can easily venn diagram your first party data with 3rd party brokers, and you can cleanroom the whole thing to get a decent venn-diagram of the overlap.

reply

mrheosuper 6 hours ago | root | parent | prev | next [–]

Why tf we allow whatever protocol was used. Like, why does my phone reply to a request for its information without letting me know ? It should be all off by default.

reply

microtonal 1 hour ago | root | parent | next [–]

You can block scanning by using e.g. WiFi client isolation or for LAN-connected devices using separate VLANs, etc.

The problem is that most ISP (modem+)routers are bottom of the barrel devices that do not allow users to configure such features. Even worse, some ISPs also scan the user's network and sell data to analytics companies [1]. This is a very good reason to always use your own router. If you want something with an Apple-like experience (mostly), Unifi gear is quite good. If you want something open source, then a router with something like OpenWrt or OPNsense + an access point with OpenWrt will do the job.

[1] https://tweakers.net/nieuws/245620/odido-router-stuurde-anal...

reply

rwz 3 hours ago | root | parent | prev | next [–]

If the device does anything with network, other devices can likely sniff a lot of information about it with high degree of accuracy based on how they react to certain network probes. But also lot of useful protocols rely on devices explicitly announcing themselves and their capabilities, like Bonjour or Chromecast.

reply

mrheosuper 2 hours ago | root | parent | next [–]

That's why i said they should be off by default. I want to explicitly tell my device to make itself discoverable.

reply

microtonal 1 hour ago | root | parent | next [–]

That's not really a good solution though. For most people, setting up devices with mDNS would be it's own kind of hell. Also, some other standards strongly rely on mDNS to even function (like Matter devices).

You need a router that allows you to configure strong policies, such as client isolation, what data can flow between VLANs, etc.

More broadly you cannot solve every with technology. The most effective route would be to simply outlaw such analytics without informed consent. This is basically what the GDPR does, but it takes a while before enough companies get fined before the industry understands. That said, the last few years, products sold in the EU are starting to get toggles to request analytics that are _off_ by default, etc.

reply

alexpotato 9 hours ago | prev | next [–]

I recently did the following:

- switch between my network and the cable router

- one port on the switch is set to "mirror mode"

- hooked up that port to a dedicated ethernet port on one of my boxes

Why do this?

Because if I run a tcpdump on that interface I see ALL of the traffic passing through the switch which includes all outbound and inbound traffic from my devices.

One interesting thing I've already discovered:

My oven sends random unencrypted keepalive messages over regular HTTP (not HTTPS) to an EC2 server.

I'm very curious to see if that changes over time.

reply

microtonal 1 hour ago | parent | next [–]

switch between my network and the cable router

One ISP here was recently caught scanning the local network on their modem/router-combo and uploading all the MAC addresses to... an analytics company.

If you have any chance to replace the ISP-provided router (in some countries ISPs are required to offer this option), do so. You can also replace it by something that has a traffic flow monitor, proper firewall (e.g. to block outgoing connections to trackers), etc.

reply

gh02t 6 hours ago | parent | prev | next [–]

See ntopng, it provides a nice monitoring UI for exactly this type of scenario. It's higher level than Wireshark, more focused on high level traffic analysis.

reply

WalterBright 1 hour ago | prev | next [–]

I have no idea why anyone would connect a coffee machine to the internet. Mine works just fine with no such connection.

reply

xdavidliu 1 hour ago | parent | next [–]

my guess is so that the company can say on the earnings call that they are going digital / going ai or whatever, "and here's 10 products we have that are taking active steps in that direction".

reply

WalterBright 1 hour ago | root | parent | next [–]

If I don't give it my wifi password, how could it connect?

reply

aabajian 7 hours ago | prev | next [–]

I recently had a delivery to my Kaiser office in Portland. It was printer ink! My printer had run out of ink. Except, I don't own a printer, and I've never owned one that self-reorders ink. Someone at some time had registered their printer to my office address and enabled self-reordering of printer ink.

reply

judge2020 6 hours ago | parent | next [–]

If it's HP Instant Ink then you probably won't get any more. After the first included set of them, you have to have those specific ones installed for it to send future refills.

reply

MarceliusK 3 hours ago | prev | next [–]

Somewhere there's an engineer who added Wi-Fi to a coffee maker because marketing wanted an app, and now a family is debugging network saturation caused by their breakfast routine

reply

matthewmcg 11 hours ago | prev | next [–]

Wow, maybe this is the push I need to finally set up an isolated "IOT" VLAN at my home.

reply

BLKNSLVR 10 hours ago | parent | next [–]

I did that relatively recently. Make sure to spend the time planning it out.

I've ended up with numerous VLANs, one for entertainment devices, one for security system(s), one for guests, one for IoT trash, etc.

If the devices are this level of untrusted, there's a lot of separation necessary.

reply

landgenoot 18 hours ago | prev | next [–]

Never assume malicious intent when incompetence.

I have multiple devices that queries their update server every 15 seconds, which all shows up as the top 10 queried domain in my network.

reply

kps 12 hours ago | parent | next [–]

Sufficiently advanced incompetence is indistinguishable from malice.

reply

Telaneo 11 hours ago | parent | prev | next [–]

It's in Kerig's interest to be evil in this case. There's money to be made in malice. There's good reason to assume this isn't incompetence.

reply

foobarian 10 hours ago | root | parent | next [–]

It could be incompetent malice.

reply

rwz 10 hours ago | root | parent | prev | next [–]

I'm sure they could've collected the same data they're collecting with 0.1% of the traffic. This particular case seems to be greed AND incompetence.

reply

GuB-42 11 hours ago | parent | prev | next [–]

There is no way it is *not* incompetence.

Considering the computing power of these kinds of devices, it is most likely stuck inside an infinite loop sending garbage at full speed, there is not enough power to process that much volume in any maliciously useful way.

reply

mjburgess 11 hours ago | parent | prev | next [–]

https://en.wikipedia.org/wiki/Plausible_deniability

reply

tombert 9 hours ago | parent | prev | next [–]

> Never assume malicious intent when incompetence.

I like Hanlon's Razor, but I think sometimes people will use it to fully dismiss the idea of someone being evil *because* they're stupid, when in reality plenty of people are capable of being both.

reply

Lammy 9 hours ago | parent | prev | next [–]

> Never assume malicious intent when incompetence.

No, fuck this lazy line of thinking. If the outcome is the same then it doesn't matter.

reply

PinkaDunka 11 hours ago | prev | next [–]

This website generated 1tb of bandwidth while serving me 1kb of text

reply

MathMonkeyMan 7 hours ago | parent | next [–]

1631 bytes of text, by my count.

Then I disabled my ad blocker to see how much data comes down. So far it's at 31 MB, but it increases without bound by a few KB per second.

reply

tintor 9 hours ago | prev | next [–]

Why does a coffee machine need internet?

reply

etoxin 9 hours ago | parent | next [–]

Or the more perplexing, a smart fridge.

Think of all that sweet sweet food data that a fridge could on sell.

reply

imp0cat 3 hours ago | parent | prev | next [–]

Exactly. Why would you even want to connect your coffee machine to the network?

reply

eek2121 7 hours ago | prev | next [–]

The only thing that I will add is that if you buy a smart appliance, you totally deserve this.

At my local home depot where I shop, there is like 1 of each type of appliance that has any type of smarts, and each one is always the most expensive. All the rest, and more reasonable, are dumb. No apps, no wifi, etc. I'm not usually a guy who cheaps out on stuff, but I also know when I'm overpaying, and would never pay $2,000 for a fridge just because it has a giant screen (and now shows ads apparently...ahem...samsung)

I have 3 Keurig coffee makers, and they are dumb as a brick.

If you buy something that can connect to wifi/the internet, please understand that you are never actually buying it. You are actually only renting it. Either you pay the price via lack of privacy, or you pay the price via subscription...and the company at the other end of the deal controls which bargain you get...you have no input.

Keurig could brick all their smart coffee makers tomorrow and demand users cough up $30/mo, and users would then have to decide on whether they should toss their coffee makers or pay up.

I'm not saying it's right. Governments aren't doing enough in this area, especially the US, but also Europe. However, that is the name of the game.

Buy something dumb and enjoy not having to worry about this nonsense at all.

reply

thedougd 6 hours ago | prev | next [–]

Time to develop an open source tarpit for these types of devices. Return data endlessly about fake network devices to overwhelm them and obfuscate your real devices.

reply

ProAm 6 hours ago | parent | next [–]

This already exists.

reply

dolmen 6 hours ago | root | parent | next [–]

Link!

reply

fragmede 6 hours ago | root | parent | next [–]

https://github.com/honeynet/EventHorizon

reply

rags2riches 3 hours ago | prev | next [–]

Who's selling a home router that isolates devices by default?

reply

microtonal 1 hour ago | parent | next [–]

In most good routers/APs (Unifi, OpenWrt, etc.) WiFi client isolation is something that is just a simple toggle (don't remember if it's on by default) and placing an SSID on a separate VLAN is also easy.

Some more consumer-oriented router/APs like Fritz!Box support a guest network that uses WiFi client isolation and internally uses a VLAN that is separate from the main network (though due to being non-pro end-user focus, you cannot set up your own VLANs or additional SSIDs).

reply

meindnoch 9 hours ago | prev | next [–]

I would require IoT devices to pass a rigorous certification process, like we do for RF devices.

reply

lifeisstillgood 12 hours ago | prev | next [–]

Holy moly - 1,747 “partners” to share my data with. I mean, how can you even find 1747 data brokers? Where do you get that list. What does the JavaScript look like - I mean … this is getting ridiculous.

But at least the EU did me a solid. I really wanted to read that but I think 2000 data scumbags is not worth the effort.

All I need know is to realise bottlecaps must be recycled and federalism is good. Repeat in the mirror each morning

reply

MiroslavPokorny 2 hours ago | parent | next [–]

How can your or mine data be worth the payment of 1747 to the advertisers ?

Advertising is a lottery, they all try to show you an ad knowing very well it will most likely be ignored.

Where do they get the money to buy your details in the first place ?

reply

CMay 8 hours ago | parent | prev | next [–]

https://texas-sos.appianportalsgov.com/data-broker-registry

reply

mahboi 9 hours ago | prev | next [–]

"Nomad explained that he had worked in IT for more than 10 years and decided to look further into what had happened."

I was hoping this post would say what happened and what kinds of packets it was sending.

reply

swader999 8 hours ago | prev | next [–]

Just imagine the devs on the other end trying to parse petabytes of data. It's breakfast on the East coast, all hands on deck.

reply

dvdyzag 6 hours ago | parent | next [–]

I'm sure Claude is allowed to take breaks.

reply

breppp 2 hours ago | prev | next [–]

I actually think this is going to get progressively better.

It's easier than ever today with LLMs to find bugs in the firmware and get complete trace of what's they are sending and shame these companies.

The next phase for the technically inclined is to patch these appliances and remove the collection, also possible today

reply

abotsis 6 hours ago | prev | next [–]

Must be all the Java bytecode.

reply

neya 51 minutes ago | prev | next [–]

Why the fuck does a coffee machine need to connect to the Internet?

reply

jttnr 11 hours ago | prev | next [–]

Maybe the coffee machine is subsidized by a residential botnet?

reply

seanhunter 2 hours ago | prev | next [–]

Also, can we talk about the fact that it is a Keurig and therefore makes disgusting swill rather than coffee.

It’s not like it was an actually good coffee machine that has an app to select espresso profiles like a Wendougee Data S or something.

reply

MiroslavPokorny 4 hours ago | prev | next [–]

Two mistakes in the title.

- A coffee machine should not be broadcasting anything. - Stop drinking coffee and go outside and enjoy the great outdoors.

reply

wolfi1 5 hours ago | prev | next [–]

question for those who use it: is it necessary to put the machine in the local network in order for it to work?

reply

jason_s 18 hours ago | prev | next [–]

`C0FFEEEEEEEEEEEEEEEEEEEE...`

reply

a96 18 hours ago | parent | next [–]

418 I'm a teapot

reply

ContinuityLab 8 hours ago | prev | next [–]

Probably because everyone is suffering from benchmark fatigue at this point. Until it handles real-world chaotic production edge cases without silent degradation, it's just another speed-run metric.

reply

nelsonfigueroa 9 hours ago | prev | next [–]

can't even make a coffee at home without being tracked

reply

ButlerianJihad 18 hours ago | prev | next [–]

A year or two ago, I was using NextDNS in ad-blocking and logging mode, which very helpfully exposed malware sitting on my very router, which had been completely undetectable, except for the veritable flood of bizarre DNS queries it was routinely sending to the self-configured DNS servers.

Now that I have a new router and I've re-enabled NextDNS, I've ironically discovered that the chief abuser of DNS right now is the router's own legit security software, which is absolutely hammering on the same query, several times a second.

Of course, since I am currently on NextDNS free tier, this matters a lot, because they cut you off after about 300,000 queries in a month. So any hammering abuse will make me lose my privileges much earlier than I would otherwise. So, to stop the abuse, should I shut off my legit security software? It is absolutely rubbish at identifying malware on the device itself...

reply

tamimio 18 hours ago | prev | next [–]

Reminds me when couple years ago I plugged the TV to the internet (so my relatives kids can watch YT) and I forgot to unplug it for almost a week after, only to find the router dns resolved (and blocked) a million queries, all from that one TV!

reply

bombcar 18 hours ago | parent | next [–]

I love when it keeps checking some random DNS address, because who knows, with a TTL of 64000 it may just have changed in the last seven milliseconds!

reply

altairprime 18 hours ago | parent | prev | next [–]

The traffic generated here is network scans, not external traffic, and so blocking DNS wouldn’t have helped.

reply

ck2 18 hours ago | prev | next [–]

it took me a month to notice my Midea A/C was absolutely hammering my router

I didn't even know it had wifi capability but it was trying to connect

I use mac whitelist so it wasn't even getting in but that didn't stop it from trying every seond

Fortunately it was just a usb dongle so yanked it out

reply

altairprime 18 hours ago | parent | next [–]

Most Midea units can be swapped for an ESPhome USB dongle if you ever wish to have remote control on your own terms — note various countries’ shop links, and the various wiki and other outlines for DIY etc: https://smlight.tech/product/slwf-01

reply

HankB99 18 hours ago | parent | prev | next [–]

Ooo. I have a Midea dehumidifier. When it powers up it displays the WiFi symbol. I wonder if it is hammering away at my access point. Might it be better to bring it on line and then just block all traffic?

And I wonder how I would even tell if it was trying to associate with my WiFi.

reply

pseudohadamard 18 hours ago | root | parent | next [–]

I have a Midea dehumidifier too. It moves around 200kB/hour which seems to be cloud polling about once a minute, so no big deal traffic-wise.

reply

jedbrooke 10 hours ago | root | parent | next [–]

it’s checking to see if they discovered a new type of water

https://xkcd.com/3109/

reply

pseudohadamard 7 hours ago | root | parent | next [–]

I actually have two dehumidifiers, one is the Midea and the second is a totally dumb Aliexpress one that cost a few tens of dollars. It's switched on and off by Home Assistant via a modbus-controlled relay and drains into a sealed water canister with a modbus water-level sensor in it. Zero-maintenance and smarter than any multi-hundred-dollar "smart" dehumidifier.

reply

ars 18 hours ago | parent | prev | next [–]

I have two of them, and I just checked and both are quiet. Mine don't connect to WiFi unless you go through an entire process first with an android phone and Matter.

It's great having them on WiFi - you can turn on the AC before getting home to pre-cool, without having to leave it on all day.

reply

sillyfluke 18 hours ago | root | parent | next [–]

Boy: So, how it get this bad grandpa?

Man: Well, before you couldn't turn on the AC before you got home

reply

ars 18 hours ago | root | parent | next [–]

Realistically people would just leave their AC on. So this saves energy, rather than changing comfort.

reply

Cpoll 18 hours ago | root | parent | next [–]

Realistically ACs have timers, so you're really only optimizing for days where you go off-schedule.

reply

seb1204 11 hours ago | root | parent | prev | next [–]

Really? And then complain about the energy cost? People are nutz. Like it's so unbearable to come home, open windows to get peak hot air out, then turn on AC and get cool. Energy is too cheap it seems. Also even very old AC remotes show there is usually the option to set up times etc.

reply

sillyfluke 18 hours ago | root | parent | prev | next [–]

I have a friend who diy'ed a button on single webpage that he presses on his phone while at work in order to open the gate to the building that he lives so delivery people can get in. I also think Bret Victor diy'ed the AC as mentioned while he was a student quarter century or more ago[0]

I know this sounds like the famous "just do it this way in linux instead" criticism of Dropbox back in the day. But I do think we reached "life parodies fiction" with these smart devices where it makes sense to give diy another go. And with AI, there's less excuses this time around I would imagine.

But I would literally rather buy a cheap phone, a cheap SIM, hotspot it and connect it to a charger and have the AC connect to that and isolate it that way instead of letting it touch the network.

[0] https://worrydream.com/Electronics/

reply

ttytty 18 hours ago | root | parent | next [–]

You can (and should) just segregate your network to have separate paths for IoT/"smart devices" and normal personal/family devices. Makes it all worry free and transparently observable.

I have my IoT on a separate VLAN and I can observe communications for any given device at any given time.. this seems like a much saner solution than outright not buying any IoT devices, though that is also a respectable decision!

reply

aksss 5 hours ago | prev | next [–]

VLANs, people. And firewall policies.

reply

gxs 8 hours ago | prev | next [–]

My biggest concern is what are we going to do when these appliances come with their own SIM card

Right now I don’t care, I just never plug anything into my network

I don’t want to have to mod all my shit just to remove data collection stuff this way

Cars already do this and it’s a bitch to disable, can’t imagine having to do it every time I buy a blender, coffee maker, knife sharpener, tv, light bulb, speakers etc etc

reply

microtonal 1 hour ago | parent | next [–]

On the other hand, when they have their own SIM card, they cannot scan or listen on your local network, so there wouldn't be much analytics to collect, except when you make your coffee I guess. Embedded SIM cards would especially be nefarious for devices like TVs. But I think most manufacturers prefer WiFi by far (more data to collect) and most customers just connect their devices to WiFi without even thinking about it.

reply

matteoraso 18 hours ago | prev | next [–]

I honestly hate the IoT so much. Why should a coffee machine of all things use data? Just make the coffee.

reply

anigbrowl 12 hours ago | parent | next [–]

I love IoT. It's the greedy corporations I hate. Everyone who implements this kinda abusive stuff, from the CEO down to the people building and installing the firmware, are scum.

reply

skupig 10 hours ago | root | parent | next [–]

Technology could be so much more useful and fun if we just fully banned the collection and sale of personal data. We've been dreaming of smart homes for, like, 80 years, but advertising ruined it just like it ruins everything. Imagine how cool it would be to able to connect devices to the internet for purely functional purposes without them spying on you!

reply

autoexec 11 hours ago | root | parent | prev | next [–]

This is all technology. Everything is being infested with spying and tracking.

reply

Levitating 11 hours ago | root | parent | next [–]

No, just pick your technology better. My LineageOS phone and framework laptop do nothing of the sort.

reply

autoexec 10 hours ago | root | parent | next [–]

LineageOS helps, like installing an adblocker helps, but there's no hope for cell phones. Your wireless provider is still tracking you and nobody knows what the blackbox wireless chipsets are doing, including your OS. Framework is a pretty good laptop (it's a candidate for my next even) if you can afford the premium. My next TV and car will be my biggest worry.

reply

goatlover 12 hours ago | root | parent | prev | next [–]

What is the need for a coffeemaker on the internet?

reply

scrlk 11 hours ago | root | parent | next [–]

A coffee maker was the subject of the world's first webcam: https://en.wikipedia.org/wiki/Trojan_Room_coffee_pot :^)

reply

linker3000 10 hours ago | root | parent | next [–]

Yeah, but the people running the Webcam probably didn't make notes about the watch / rings / shirt / dress / shoes worn by the people using the coffee maker, nor take down whether they were wearing glasses and if they added milk - and sell this information to the local jewelers, clothes shop, shoe shop, opticians and dairy.

Probably.

reply

anigbrowl 9 hours ago | root | parent | prev | next [–]

https://en.wikipedia.org/wiki/Fallacy_of_composition

reply

robotnikman 12 hours ago | root | parent | prev | next [–]

The shareholders as well.

reply

j45 10 hours ago | prev | next [–]

A great reason to limit “Smarthome” devices to a dedicated guest or iot wifi network.

reply

m4rtink 7 hours ago | prev | next [–]

So is finally someone going to jail for another insanity like this ?

reply

ButlerianJihad 18 hours ago | prev | next [–]

Last year I had a big dispute with my ISP that was refusing to support or provide proper WiFi on their router, even while they touted a trademarked brand-name to do it. I ended up turning their router into Bridge Mode and purchasing a real router that could do WiFi. I did this extremely reluctantly, because every other personally-owned router had contracted malware.

After installing the new router (Netgear) my HP LaserJet began printing error pages. Like, I had done nothing to send anything to it, but a blank error page or three would pop out of it at very random times.

It took awhile to narrow down and diagnose this. But it turned out that the Netgear system had a very... proactive network malware detection system. It was red-team scanning my LAN for "vulnerabilities" or exploits or the presence of malware (I think just known vulns). It was a known side-effect of these scans, where it would tickle an RTSP TCP port of some kind and the HP printer would respond with its error printout.

I was *so livid* that the router was scanning the LAN, basically unbidden and completely undocumented. Even worse, they were not sharing the logs or results of that scan with the consumer. No, they were being sent back to the Netgear mothership, and their cybersecurity vendor overlords. So the scans were not designed to benefit me; they were simply designed to spy on everyone from a privileged vantage point. Now I ask you, why is a piece of kit that is supposed to be "yours" compiling secrets about your network, hiding them from you, and turning them over to, I guess a big database for hackers to leak in due time? This is not a question of "well, devices hooked up to a network should not be vulnerable" if the devices were contained in a private network, and 100% inaccessible from outside, and only attackers inside my perimeter could do these exploits in the first place.

Thankfully I found a way to disable this. Their "security" shitware is still spamming DNS and I may be forced to disable that as well. Meanwhile, routers 100% cannot self-introspect or self-diagnose and find their own malware. I've said it once; I'll say it again: consumer routers are the Achilles Heel to your network. They are ideal points of compromise for any actor to gain a foothold and pivot, or simply gain persistence undetected. Your ISP doesn't care, and your vendors don't care. Perhaps you should.

reply

freecodeio 10 hours ago | parent | next [–]

If my printer printed random shit I would just get paranoid and wipe every piece of tech clean. But good on you for discovering why though.

reply

mrheosuper 5 hours ago | parent | prev | next [–]

Why not setup opnsense/pfsense/openwrt on a small PC. You already went with your own router

reply

ButlerianJihad 2 hours ago | root | parent | next [–]

One of the routers I had in the distant past, which I flashed with some kind of OpenWRT, was clearly pwned. I do not know if the firmware I downloaded was pre-compromised, or if some entity pwned it as soon as the Internet was accessible. But I would not trust OpenWRT or Tomato or whatever with that track record. I do not need or want such complexity. I want an appliance router that works and will not cause me headaches. In fact, I purchased and evaluated a "gamer router", I believe it was from ASUS, that was extraordinarily complex, and had amazing bells-and-whistles, but ultimately it was not appropriate for home use. That headache-free, simplistic appliance was supposed to belong to my ISP, but they consistently refuse to provide one to me that is fit for purpose.

reply

mrheosuper 2 hours ago | root | parent | next [–]

I believe many vendor Firmware is just OpenWRT under the hood.

If you don't trust prebuilt binary blob, just build it yourself. At least you have option.

reply

AngryData 18 hours ago | parent | prev | next [–]

Wow that seems bonkers to me. Basically scanning and cataloging known vulnerabilities on the sly, and when anyone notices they pretend it is for your benefit somehow.

It would be like finding out ring cameras are taking pictures of your keys and calculating the pin set to producing duplicates and sending that pin set data off somewhere and when caught them being like "Uh, we are uhhh... doing it to make sure your key isn't too worn down or to detect if someone made a crude hand filed key. Yeah that's it!"

reply

rendall 18 hours ago | prev | next [–]

The GDPR consent form on this blog did not have a “Reject all” button. It required me to manually reject 16 instances of “legitimate interest,” then scroll through 1,746 vendors to make sure they were all set to reject.

Seems worth mentioning in a post about excessive and intrusive collection of user data. The moral outrage rings hollow when opting out of tracking is so deliberately onerous.

reply

wafflemaker 18 hours ago | parent | next [–]

And also illegal. It's illegal not to have one button. Companies didn't do it because they suddenly stopped being scum.

reply

realaaa 11 hours ago | prev | next [–]

ahahahah that's gold !

IoT network yep, needed yesterday

reply

moron4hire 8 hours ago | prev | next [–]

So now I need a second revolver to put next to the coffee pot? Or do you think I should just relocate the printer next to the coffee pot so I only need one?

reply

bitwize 12 hours ago | prev [–]

As another sign of the enshittified world we live in, the thing probably wasn't even RFC 2324 compliant.

https://datatracker.ietf.org/doc/html/rfc2324

Bruh should have set his PiHole to return HTTP 418 in response to any outbound request this thing made.

reply

Consider applying for YC's Winter 2027 batch! Applications are open till November 2.