DESPITE PETE HEGSETH, SIGNAL IS GOOD

Why you should use Signal (But *maybe* ditch Whatsapp?)

Pete Hegseth is Bad at His Job

The Secretary of Defense and Fox Host Pete Hegseth keeps using Signal to talk about war plans with people he's not supposed to be talking with at his day job. He also gets caught, because he's bad at security as well as his job. Hegseth uses his personal phone for Department of Defence business, including killing a lot Yemenis.

What Hegseth was supposed to use instead of his consumer cell phone is a SCIF, or Sensitive Compartmented Information Facility. I've been in one. I was emphatically invited to leave my phone at the door. There were large men making this point to me, and I took it to heart. A SCIF *is* secure, but it is as much about control and legal obligations as it is about security, and rightfully so. Secure communications for a national government don't just require security, they require accountability, integrity, and a durable record. After its classification period, that information belongs to all Americans. Historical accountability is something we've decided matters, and encoded into our laws.

On a technical level I wouldn't be shocked if SCIFs use some of the same technology that's in Signal to secure communications. It's good stuff! But SCIFs are SCIFs, and consumer cell phones are cell phones. Your phone is not

designed for government records retention, or hardened against specific nation-state threats. But modern, up-to-date phones have very good security, more hardened then most of the government systems that have ever existed. And it's right there! In your phone without you having to do anything to get it! (Except apply new software updates when they turn up.)

So despite the fact that Hegseth's phone *would* be one of the more targeted in the world, and Hegseth himself is an idiot, his phone isn't necessarily compromised. It might be, but it's hard to be sure. It's quite hard to hack a modern phone, especially if the person using the phone updates it every time there's an update released, and doesn't click on things they don't know are OK. There are fancy attacks, called Zero-Click Attacks, that don't require any user interaction, but they're hard to build and expensive.

At any given moment, you don't know whether someone had a working attack against an up-to-date iPhone or Android until it's discovered and patched. But mostly, the average user doesn't have to worry about trying to secure their phone. You already secure your phone when you update it. The hackers aren't in a race with you, or even Pete Hegseth, they're in a race with large and well-funded security and design teams at Google and Apple – and those people are very good at their jobs. This is why the nerds (like me) always tell you to update software as soon as possible; these updates often patch security holes you never knew were there.

You're more likely to download a vulnerability in something like Candy Crush, weird social media apps, or random productivity tools you're tying out. But the folks at Google and Apple have your back there, too. They've put every app into its own software-based "container," and don't let apps directly interact with the core functions of your phone, or the other apps on it. Hackers try to break out of these containers, but again, it's not easy. Even if

they get a foothold in one, they might know a lot about how good you are at subway surfing, but not much else.

It’s hard out here for a phone hacker.

Sometimes the hackers hit pay dirt, and find some flaw in phone software that lets them take over the phone from the air, with no user interaction — that zero-Ccick attack. This is very scary, but also very precious for the hackers. Unless there’s a very good reason, no one is going to risk burning that bug on you. If an attack like that is found, it will be top priority for those big smart security teams at Google and Apple. There will be long nights. There will also be an update that fixes it; *apply updates as soon as you see them*. Once a vulnerability is patched, the malware companies have to go back to the drawing board and look for another bug they can exploit to get their revenue stream back.

The high profile malware companies often sell their software, especially if they have a zero-click attack, to governments and corporations. They don’t want normal people using it, because the more it gets used, the faster they will be back at square one after Google and Apple take their toys away.

Nerd’s Delight

Signal is usually the favorite app your exhausting nerd friend keeps badgering you to download. It’s risen to even more prominence due to Pete Hegseth’s repeated idiocy. But this has caused doubt and confusion, because if you found out what Signal was from Hegseth’s leaks and

blunders, it doesn't look so good. Using Signal for DoD high level communications is not only illegal, it is stupid. Signal isn't meant for government classified communications.

But it *is* meant for you, and it's very good at what it does.

Signal is two things: First, an app for Android and iPhone (with a handy desktop client) which encrypts chats and phone calls. That's the Signal app you see on your phone. second, the other part is the Signal Protocol, Signal's system of scrambling communications so that people *outside* of the chat can't see or hear anything *inside* the chat.

Signal Protocol, the encryption system Signal uses, is a technology called a Double Ratchet. It is an amazing approach that is pretty much unbreakable in a practical sense. The very short version of how that encryption works is this: Your computer finds a special number on a curve (think of the pretty graphs in trig class) and combines this number with another number the other person has, from a different spot on another curve. These numbers are used to encrypt the messages in a way that only you both can see them. (This number generation is done by your phone and servers on the net in the background of your chat, and you never have to see any of it.) You each use the numbers from picked out these curves to encrypt a message that only the other person can read. Picking out the number from the curve is easy, but guessing it from the outside is functionally impossible. Any attempt to figure out the points on the curve you used is very hard and tiring – meaning it takes the computer a lot of energy to try. In computers, very hard always translates to expensive and slow. The extra trick in Signal's double ratchet is a mechanism for taking that already hard number to guess and "ratcheting" it to new hard numbers – with every single message. Every Hi, Whatup, and heart emoji get this powerful encryption. Even if someone was using super computers to break into your chat (and they

aren’t) every time they broke the encryption, they’d just get that message, and be back at square one.

That’s expensive, frustrating hard work, and your chats aren’t worth the bother.

The Strongest Link, Weakened?

Messenger also uses the Signal protocol

Whatsapp adopted Signal Protocol in 2014, granting encrypted privacy and safety to over a billion people.

Signal is secure. Whatsapp and Facebook Messenger use Signal protocol too, and are also secure, for now… but Meta has made some decisions that complicate things. In a rush to add AI to everything whether you want it or not, Meta has added AI to its Signal Protocol-secured chat rooms. This doesn’t break the Signal Protocol, that works fine. But to have AI in chats means that by definition, there’s another participant listening in your chat. If there wasn’t, it couldn’t reply with AI things. If

you’re not comfortable with this, it might be time to ditch Whatsapp and Facebook Messenger for Signal.

I’m personally not comfortable with it, in part because as far as I can tell, there’s nothing technically or legally stopping law enforcement from demanding access to that listening function in any chat room. It may only give the police access to parts of the conversation, but I’d like the chance to defend my data myself if it comes to it. I don’t want to have it picked up from a third party without so much as notice to me.

Meta is in the the room with you, like it or not. Is it recording all your chats somewhere? I doubt it. It’s a bad idea that would make too much trouble for Meta if it got out. But I can’t know for sure. I know there’s no listener in Signal, because the protocol makes hiding a listener functionally impossible. (To be clear, Meta isn’t hiding it, they’re advertising it. But it’s still a listener.)

Encryption for All

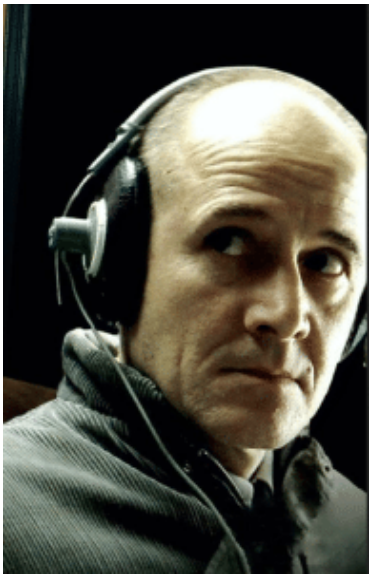
Make no mistake, that Whatsapp and Facebook Messenger use Signal’s protocol is wonderful news. It means that, without having to know anything about internet or computer security, one day there was an update, and billions of users got to rely on some of the best encryption ever designed, without even knowing it. This is important both for keeping people safe online, and for making society better, as activists, small businesses, families, and everyone with and internet connection can talk freely and safely to their people and their communities. It doesn’t stop ill-intentioned people from doing bad and deceptive things like lie, cheat, and steal, but it makes it harder for them to enlist the computers into their schemes.

The problem with Pete Hegseth using Signal is two-fold: He has to retain records legally, and ratcheting encryption is intentionally

ephemeral. Signal is the worst way to retain records, beyond perhaps toilet paper and sharpie. The second problem is that if he does have a vulnerable app on his phone, or there's a general vulnerability the teams at Apple and Google haven't found yet, someone could be listening into what his phone is doing. Maybe even through his Candy Crush Saga, a fun game you will never find in a SCIF, no matter how much you wish you could.

SCIFs are kind of boring. No phones, the windows are weird (to defeat directional mics) and in my case, I had to have security escort me to the bathroom. I imagine that's why an exciting guy like Hegseth doesn't use them. But he is not only putting people in danger with his shenanigans, he's also robbing the American people of a record that is, by law, our right to have. And it's looking like an era of American history in which we want to be preserving evidence.

The Online Lives of Others



If you've never seen the movie The Lives of Others, go watch it. It's great, and annoyingly relevant right now.

There is another threat coming from the EU and UK that rears its head every few years, and probably from the US soon enough as well. Many governments and law enforcement agencies want, have wanted for years, a scheme digital rights advocates call Chat Control. Law enforcement would have a back door into everyone's encryption, usually a listener, like the Meta AI, but much worse. It would bug all chats – a spook in every phone. The excuse is always CSAM, or Child Sexual Abuse Material, but the proposal is always the same – to strip every person of privacy and the technical means to protect it, in the name of protecting children. This ignores a lot of of issues that I won't go into here, but suffice to say the argument is as dishonest as it is ineffectual.

It's an ongoing fight pitting children against a right of privacy and personal integrity, and it always will be an ongoing fight, because it would give the police and governments nearly limitless power to spy on the entire populous all the time.

Total digital surveillance is simply not a feasible way to run a society. It is the police state the East German Stasi dreamed of having. It must be resisted for human decency and flourishing. Let's give the totalitarian desire for a spy in every phone no oxygen, it has no decency, no matter who it claims to be protecting.

Even if you never do anything that could be of interest to governments or law enforcement, using encryption creates more freedom for all. If only "criminals" or "enemies" use Signal, then using Signal becomes a red flag. If everyone uses Signal (or Signal protocol in Whatsapp/Messenger), then it's normal. You get the measure of protection it provides from scammers and hackers, and you help people fighting criminals and resisting tyranny, all over the world. This is one of the reasons adding Signal protocol to the Meta systems was such a great moment in the history of the net. A

good portion of humanity gained a real measure of privacy that day.

If activists and people “with something to hide” are the only people using encryption like Signal, it’s grounds for suspicion. But if everyone is using it, the journalists and activists who need it for political reasons don’t stand out. The battered partners and endangered kids can find it and use it safely to get help. And everyone is safer from scams and hacking attacks — because what you do and say has some of the best protection we’ve every conceived of as a society, even if it’s just your shopping list.

Correction: A previous version of this article included a description of Diffie–Hellman key exchange in the explanation of how Signal’s encryption works. Signal changed from Diffie–Hellman to Elliptic Curve Cryptography, which is much more efficient, in 2023. I regret the error.