Tell HN: I asked Signal motivations for SMS removal

56 points by quentinus95 1 hour ago | hide | past | favorite | 7 comments

Here is their answer:

Hi,

Thank you for your thoughts on the announced SMS removal. The blog post describes all of the biggest factors in making this decision, but I know this is a change that is difficult to adjust to, so I wanted to chime in with some additional info that might give some more context.

1. RCS (Rich Communications Services) is coming, and it doesn't play well with Signal. I once had a situation when I was sending SMS to one of my friends via Signal, but I wasn't seeing any of their responses – this was because their app was automatically responding via RCS, which wasn't delivered to Signal. This is going to continue to get worse, and Signal cannot add RCS support because there's no RCS API on Android. Honestly, the days of any third-party SMS app are numbered.

2. Proper SMS/MMS support is hard. Signal has to support thousands of devices running dozens of versions of Android. Now multiply that by the hundreds of cell carriers running an inherently bad/buggy protocol, and you'll start to understand the weird MMS bugs we can run into. And any time spent trying to fix them is time invested in an insecure protocol.

3. SMS/MMS has plenty of its own bugs. Remember that incident a few years ago in which everyone got old Valentine's SMS messages delivered 9 months later? It was an SMS protocol bug for which some users blamed Signal. Other weird bugs like temporarily-split MMS groups, bad image quality, and the general inability to leave MMS groups are flaws in MMS that also get attributed to us.

4. Spam. My goodness, SMS spam is a real thing, and many people who use Signal cannot tell the difference between SMS spam and Signal messages if both come through Signal. They think we're responsible for the spam.

5. Finally, Signal having SMS support gives a lot of people the wrong impression of SMS. They think that because SMS is being sent through Signal, it's actually secure or as secure as an encrypted Signal-to-Signal message, and that's just not true. We can add unlocked padlock icons to each SMS message, and we can label the message compose box as "insecure", but the misunderstanding would continue. The only thing we can do is store the SMS messages encrypted on the device, but in my opinion that matters very little when anyone who wants your SMS messages can just get them all from your cell carrier.

In short, SMS is on its way out in general, and in a world where Signal supports SMS, all of SMS shortcomings are often attributed to Signal itself, all while confusing people into thinking their SMS messages are secure.

In my opinion, a secure SMS app does not exist. Just choose the one with the best layout or usability, and preferably one that supports RCS (which I believe at this point are Google and Samsung Messages), because at least then there's some chance that they might end up being encrypted in the future.

I hope that helps give some more context. And please know that I understand this is difficult to adjust to. I can relate. I've used Signal as my SMS app for over 6 years, but I truly think it's for the best.

add comment

foepys 29 minutes ago | next [–]

Turning RCS into their own private messaging platform on Android has to be peak Google.

They tried to make a bazillion messenger apps, all of which failed, and now they try to piggyback on an existing standardized protocol but don't expose any APIs for other apps.

reply

girvo 12 minutes ago | parent | next [–]

> *Turning RCS into their own private messaging platform on Android has to be peak Google.*

While at the same time pushing this "Apple is bad because green bubble" narrative because Apple doesn't support it. It's somewhat amusing in some ways. Companies (Google or Apple) are never on the consumers side, and yet we fall for it all the time.

reply

hocuspocus 4 minutes ago | parent | prev | next [–]

And it's not only on the client side, but also server side. There are carriers who implemented Universal Profile on their own and cannot connect to the ones running Jibe. So much for a federated protocol.

So today it's either Google or Samsung messages and Jibe, otherwise RCS is essentially useless. From what I know Facebook wanted to get on board at some point, I'm not sure why this didn't work out.

The fact Google publicly whining about the iMessage lock-in is pretty rich.

reply

tao_oat 18 minutes ago | prev | next [–]

Thank you for sharing this; this is very useful context. I wonder if it would have reduced the outcry from their initial blog post if they'd included these examples.

reply

bestouff 11 minutes ago | prev | next [–]

That should have been written into the blog post. Not the current tasteless PR.

reply

captainmuon 23 minutes ago | prev [–]

Tangential, but to 1.: Isn't RCS just built upon TCP/IP and SIP? Why can't you just implement it in user space? Or does it need to send some magic packets through the modem? It is really hard to find details on the protocol.

reply

arianvanp 8 minutes ago | parent [–]

Another problem is that Google's RCS implementation has a Signal-protocol prekeys-exchange server in the loop that is not accessible for the public. So even if you'd implement RCS you could not send messages to android devices as you can't fetch the prekeys through anything but the Messages app.

reply