I Tried the Privacy Phone Network Intended to Mask Your Identity

10-12 minutes

Hacking. Disinformation. Surveillance. CYBER is Motherboard's podcast and reporting on the dark underbelly of the internet.

On Friday, 5142 were the last four digits of my IMSI, the unique code linked to my SIM card, according to an app on my phone. This code is what telecommunications giants and surveillance vendors often use to track phones, and by extension people, as they go about their business.

In the app I then pushed a “Change ID” button. About a minute later, my IMSI had changed. The last four digits were now 5206, the app said. To third-parties that might snoop on IMSIs, such as those that use a suitcase sized piece of spy tech called an IMSI catcher which hoovers up the unique codes in a certain area, or a network that might give data related to that IMSI to the authorities, I might as well be a new person altogether, depending on the capabilities of the device.

This is PGPP, or Pretty Good Phone Privacy, a new pseudo-phone network that aims to add an additional layer of privacy on top of traditional and surveillance heavy telecommunications networks. The tool certainly does not solve the issue of privacy on phones as a whole—that problem is complex, with multiple parts such as the operating system, the hardware, and more—but it could help protect against the sort of persistent surveillance that everyone is subjected to by simply being connected to a phone network.

In my testing it seems the service might be suited to those who want to add an extra layer or two of protection to their data and identity when using mobile phone networks. PGPP probably won’t help entirely against targeted attacks—the developers are clear in that this is not the intent. But if you want something that lets you use phone networks a little more comfortably, PGPP could be an interesting, if still in early stages and sometimes buggy, option.

> ***Do you know about any other privacy focused phones, or new methods of phone tracking? We'd love to hear from you. Using a non-work phone or computer, you can contact Joseph Cox securely on Signal on +44 20 8133 5190, Wickr on josephcox, or email joseph.cox@vice.com.***

“Our aim is to thwart current bulk data collection in the network, which have centered around IMSIs and IPs,” Paul Schmitt, a researcher from Princeton University and who is behind PGPP along with Barath Raghavan from the University of Southern California. The pair presented research on PGPP

at the respected Usenix Security Symposium last year and have now rolled out PGPP as a beta. “We believe that PGPP raises the bar significantly for mobile privacy,” Schmitt added. The pair are offering PGPP under the company name INVISV.

On the user side, PGPP comes in the form of an app. A user downloads it, pays for a subscription, and then runs through a mostly automated setup process which downloads an eSim to their phone. An eSim is a digital SIM card; instead of having to place a physical card inside the phone, the device downloads all the necessary information online. From there, the user is connected to the PGPP network and can change their IMSI as they please in the app a certain number of times every month, depending on their subscription. The Pro plan is $90 a month and includes 30 IMSI swaps per month with unlimited data, and the Core plan costs $40 which includes 8 IMSI swaps and 9GB of data. That’s it, you don’t pay a more traditional carrier on top of that.

Many Mobile Virtual Network Operators (MVNO) exist, which are companies which sell telecommunications service but use the infrastructure in place of more traditional mobile network operators. PGPP isn’t either one of those. Schmitt framed it more as an eSIM app. INVISV buys eSIMS from Telna, a telecommunications service provider based in Canada, which in turn has agreements with mobile operators in various countries, Schmitt explained. Telna, for example, receives a pool of IMSIs from the Polish telecom Play. When Motherboard started the signup process for Signal, the app autopopulated the number to receive a verification code with the Polish +48 country prefix. Since phones on the PGPP network don’t technically have phone numbers, users would need to find another way to sign up to Signal on such a device (Raghavan said INVISV is going to add an inbound-only SMS service for this sort of verification). Motherboard successfully downloaded and had multiple voice calls on Wickr, another encrypted app now owned by Amazon.

Beyond the protections PGPP offers around IMSI swapping, the service is bundled with a second part which INVISV calls “Relay.” This is closer to something like Apple’s recently announced “iCloud Private Relay,” which sends users’ internet traffic through two points before reaching the wider internet, hiding the users’ IP address and some other information from third-parties. The iCloud Private Relay is only for when users browse the web in Safari and, obviously, only applies to Apple devices. PGPP’s Relay meanwhile “provides whole-phone two-hop IP privacy,” Schmitt said.

“Like Apple, we partner with Fastly for the second hop that egresses onto the Internet. With Relay we wanted to make something that just works and can be used by anyone and provides more protection than a VPN (since VPNs are architecturally centralized, not decoupled, so they are controlled by a single company with a single point of observation),” he added.

Together, the IMSI swapping and Relay provide a set of tools that will generally increase users’ privacy on the internet to some degree.

If the feds come knocking and ask for PGPP user data, INVISV says it will not have much private information to give in response to any data requests.

“We've talked through this with our lawyers in preparation (we're too small to have lawyers on staff/in-house counsel)—our process is to evaluate whether the request is an actual legal order that we are mandated to comply with, and only if that's the case we proceed to the next step which is to consider the content of the order. We have very little information that we could provide, and this largely has to do with the decoupling we designed into the system,” Schmitt said.

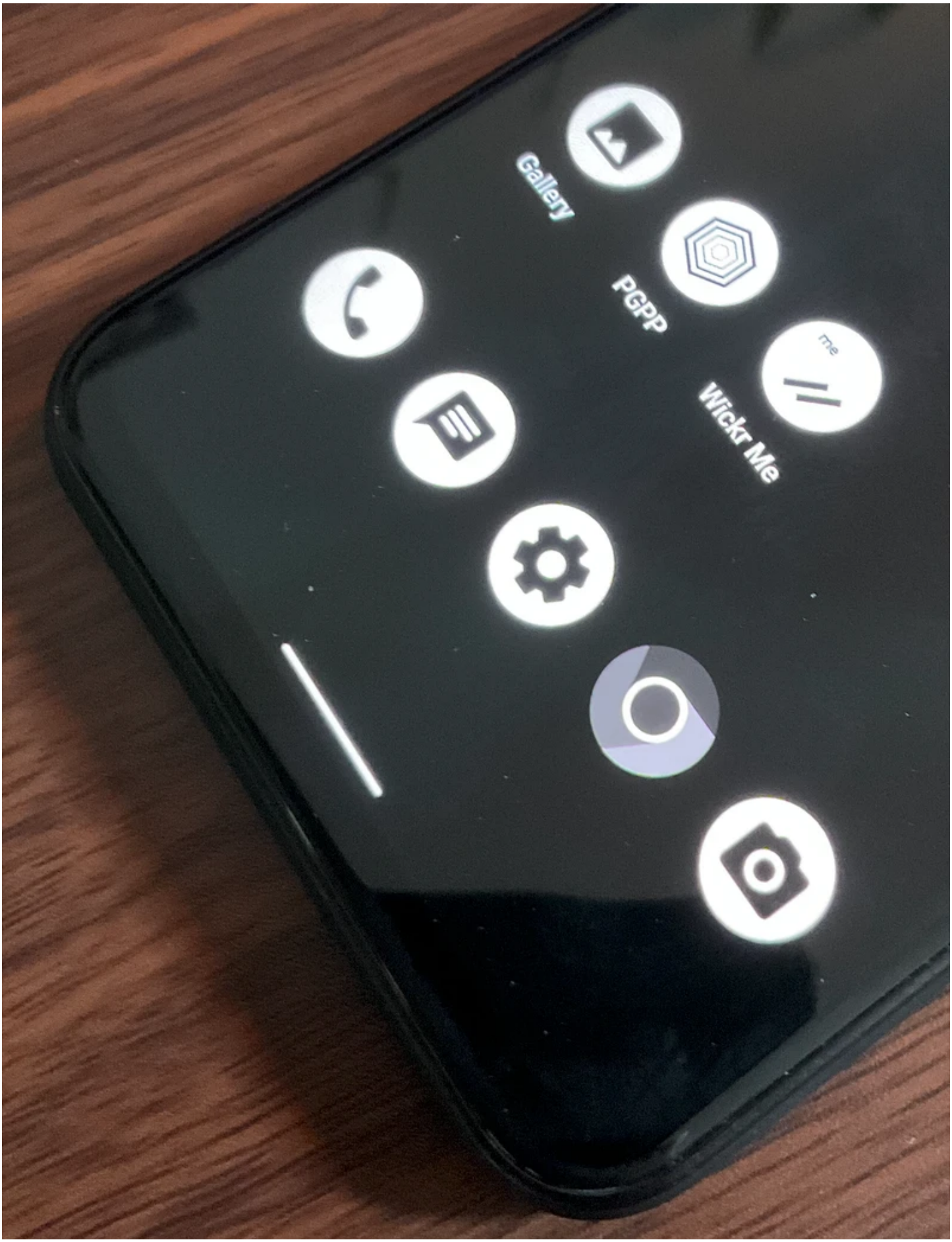
INVISV is able to see partial credit card information and when the subscription was paid for, as part of their use of the payment processor Stripe, Schmitt said. “But we don't know any identifying information about the phone from which the subscription was made (the user can do it while on a VPN, at a public WiFi hotspot, etc.).” Raghavan added it is possible for users to pay with a prepaid card if they choose to. These can be sourced with cash, creating another layer of obfuscation on the user’s identity.

“Common (as far as we know) agency requests are along the lines of ‘provide us information about this IMSI | MSISDN [phone number] | IP address.’ We do not have useful information for any of those three,” Schmitt said.

Agencies could try to obtain information from other parties, such as underlying telecommunication companies that have the infrastructure that PGPP is piggybacking off. And ultimately, each device still has an IMEI. These are different from IMSIs, in that they are a unique code baked into each phone, and which, depending on the situation, can be used to identify a device.

“They are likely to be able to get some data that way [by going to the telecommunications companies]—more than we have—but we believe we have made it harder for bulk collection to take place. Mobile operators sometimes query for IMEIs to check against the stolen handset database, and this happens from the mobile core straight to the baseband chip on the phone, which is outside of what we can control,” Schmitt said, and added that for bulk tracking “IMSIs are currently used for this, along with phone numbers (MSISDN). This doesn't mean that the IMEI couldn't be used this way in the future, but it takes a long time for big mobile operators to adapt to new technologies.”

Karsten Nohl, a security researcher at SRLabs who has focused on telecommunications security told Motherboard in an email, “The mobile network can still track based on IMEI.”



PGPP of course does not address other data collection from mobile phones that is independent of the phone network itself, such as that done by the Google Android operating system. Over the past several years, law enforcement agencies have increasingly served so-called reverse location data warrants against Google, where officials request information on all devices that were at a particular

location at a specific time. This information is gleaned from Google itself and the location tracking capability inside Android.

So to mitigate that I then installed PGPP on a GrapheneOS phone. GrapheneOS is a heavily re-engineered version of Android that strips out much of the operating system's capability for surveillance. By default this also includes the Google Play Store, but users can download that to access apps if they want to. Raghavan sent me the APK of PGPP itself to install so I didn't have to grab it from the Play Store, but most users would need to do this or download it from a third-party site.

The only tweak necessary to run PGPP on a GrapheneOS phone was that I needed to "enable privileged eSIM management," a toggle in the GrapheneOS settings. Daniel Micay, who is behind GrapheneOS, told me that eSIM activation does partly use a Google service, but that "it's not a risk beyond the fact they are aware of that device activating eSim."

When asked about the benefits of PGPP more generally, Micay said he thought "it would only be useful if you kept switching phones to get new IMEIs."

Swapping phones constantly is an extreme position though. For someone who wants to introduce extra friction to a third-party being able to identify their phone activity to their real identity, PGPP can still provide some of that.

"This is actually something I've been wanting for a while, I've been using a data only plan from T-Mobile, but as many privacy advocates will point out it's not really helpful because of IMSI tracking," Lucky225, a phone phreak and privacy advocate who has previously found gaping security issues with telecommunications networks, told Motherboard in an online chat.