**Would you pay $19/month to completely secure your online privacy?**

**<image 1>**

This is the question being asked by a new brand of personal security company that offers “privacy-as-a-service”. This type of service, whereby you pay a monthly fee to use a sophisticated system that completely anonymises all online data about you, is gaining in popularity, both with enterprise clients and now with domestic users as well. Dispel, one of the more progressive of these service providers, has just launched its secure platform for Android phones.

Dispel emerged out of obscurity late last year when it publicly announced its platform, providing everything from $19/month to $199/month plans to corporate clients. The move to Android was seen as a natural evolution to not only better serve corporate clients but also to meet the needs of a public increasingly sensitive to issues of online privacy and security.

**<image 2>**

As Dispel CEO, Ethan Schmertzler, told me, “The workforce is no longer sitting in a single building at fixed workstations, behind firewalls and routers. They’re in cafes, airports and hotels on Android phones.”

Those following the recent [Apple vs FBI debate](http://www.androidauthority.com/fbi-hacks-san-bernardino-shooter-iphone-682745/) on encryption would be well aware that government efforts to unmask and investigate bad actors involved in cybercrime, drug trafficking and terrorism also have [massive potential to affect individual privacy](http://www.androidauthority.com/the-dark-side-of-encryption-672851/) in dramatic ways.

“Encryption solves the problem of the content of what you’re communicating…but what it doesn’t do, and can’t do, is protect the context around what you’re doing: who you are, where you are, what you’re doing, who you’re talking to and when you’re meeting them. That metadata is what Dispel’s service offerings protect.”

**<image 3>**

How “privacy as a service” works

The way Dispel’s platform works is complex, using existing global cloud-based providers to host various components of Dispel’s infrastructure. When you wish to transmit data using the service, those components are temporarily assembled from unpredictable locations just long enough for your data to be transmitted and then destroyed.

The IP address used for the transmission is re-assigned to someone else and there is no trace kept of the data transmission. Dispel stores no metadata about its users, only maintaining basic records required for billing purposes. Because there is no paper trail or evidence of the service once it has been used, there is nothing for bad actors, governments or others to track.

**<image 4>**

No safe haven for bad actors

As Schmertzler notes, “Without taking a stance for or against the Snowden releases, they were a watershed moment for individuals as well as companies…. The government actions that were detailed in Snowden’s documents really crystallized for everyone – individuals as well as CIO’s of companies – that if the U.S. Government is doing this kind of thing, that other foreign governments are doing exactly the same sort of things, if not more.”

If the U.S. Government is doing this kind of thing, other foreign governments are doing exactly the same sort of things, if not more.

But Schmertlzer is quick to point out that Dispel is actively working against its service being adopted by bad actors as a haven for nefarious interactions. Dispel maintains an industry-standard black list of sites that won’t be honored if an attempt is made to access them. Dispel won’t keep a record of the attempt but the connection won’t be made either.

**<image 5>**

Do I need “privacy as a service”?

Dispel essentially offers enterprise-level security to the Average Joe. But if you’re wondering why on earth you would need that level of security, Schmertzler has an answer that’s hard to argue with: “Mobile devices carry an immense amount of information about who we are and what we’re interested in. Our entire lives are basically being captured in them.”

Mobile devices carry an immense amount of information about who we are and what we're interested in. Our entire lives are captured in them.

Paying $19/month on top of your existing data plan or ISP arrangement certainly won’t appeal to everyone, but for anyone sincerely interested in protecting themselves from identity theft, cybercrime and other online threats, it may just be a small price to pay for peace of mind.

**<image 6>**

Dispel’s plans are data capped too, not limited to specific devices, so you can use the service on all your devices and only have to worry about the bandwidth you’re using. You can try Dispel’s service out for free for three days via the Android app linked below. The app is incredibly straightforward, essentially providing a one-click solution to online security.

[**INSTALL DISPEL**](https://play.google.com/store/apps/details?id=io.dispel.android) https://play.google.com/store/apps/details?id=io.dispel.android

How seriously do you take your online security? Would you be willing to pay for complete privacy?