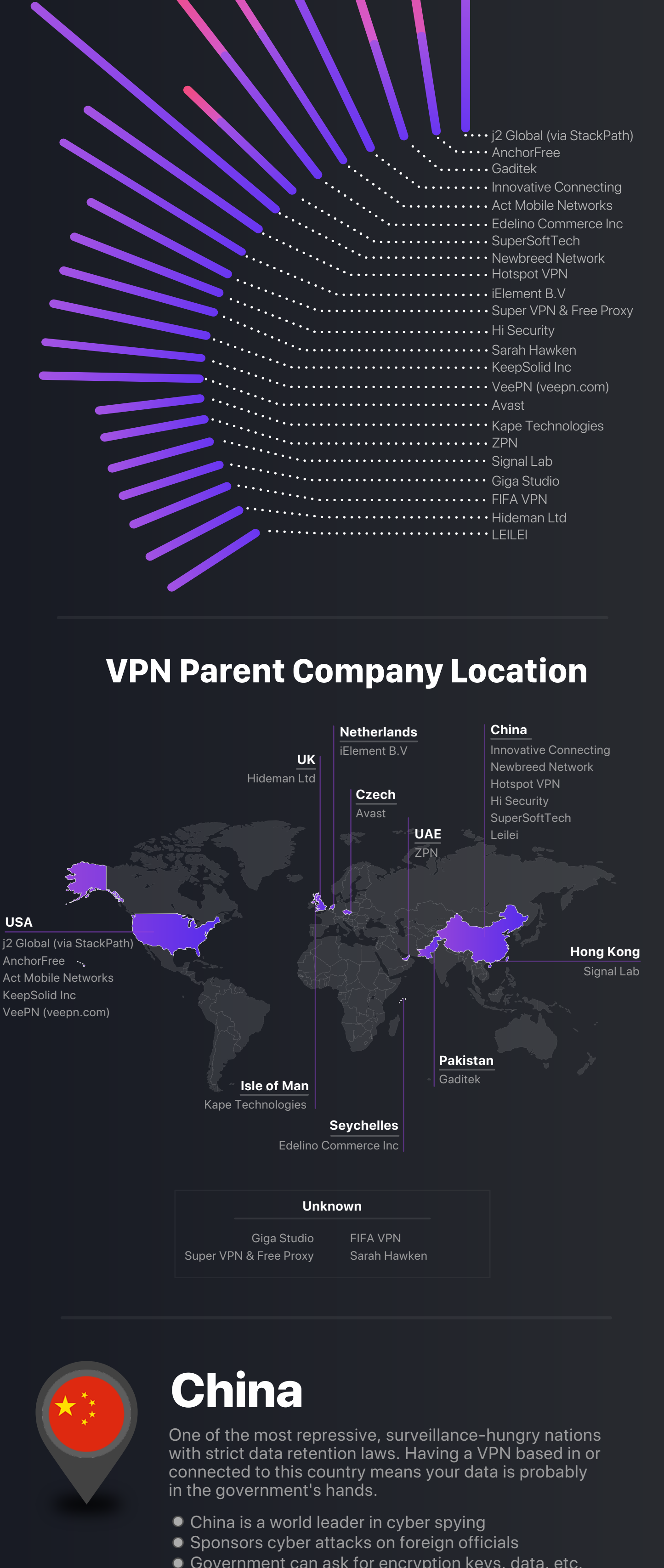
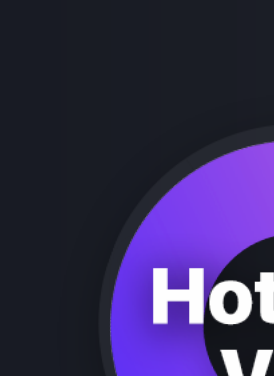
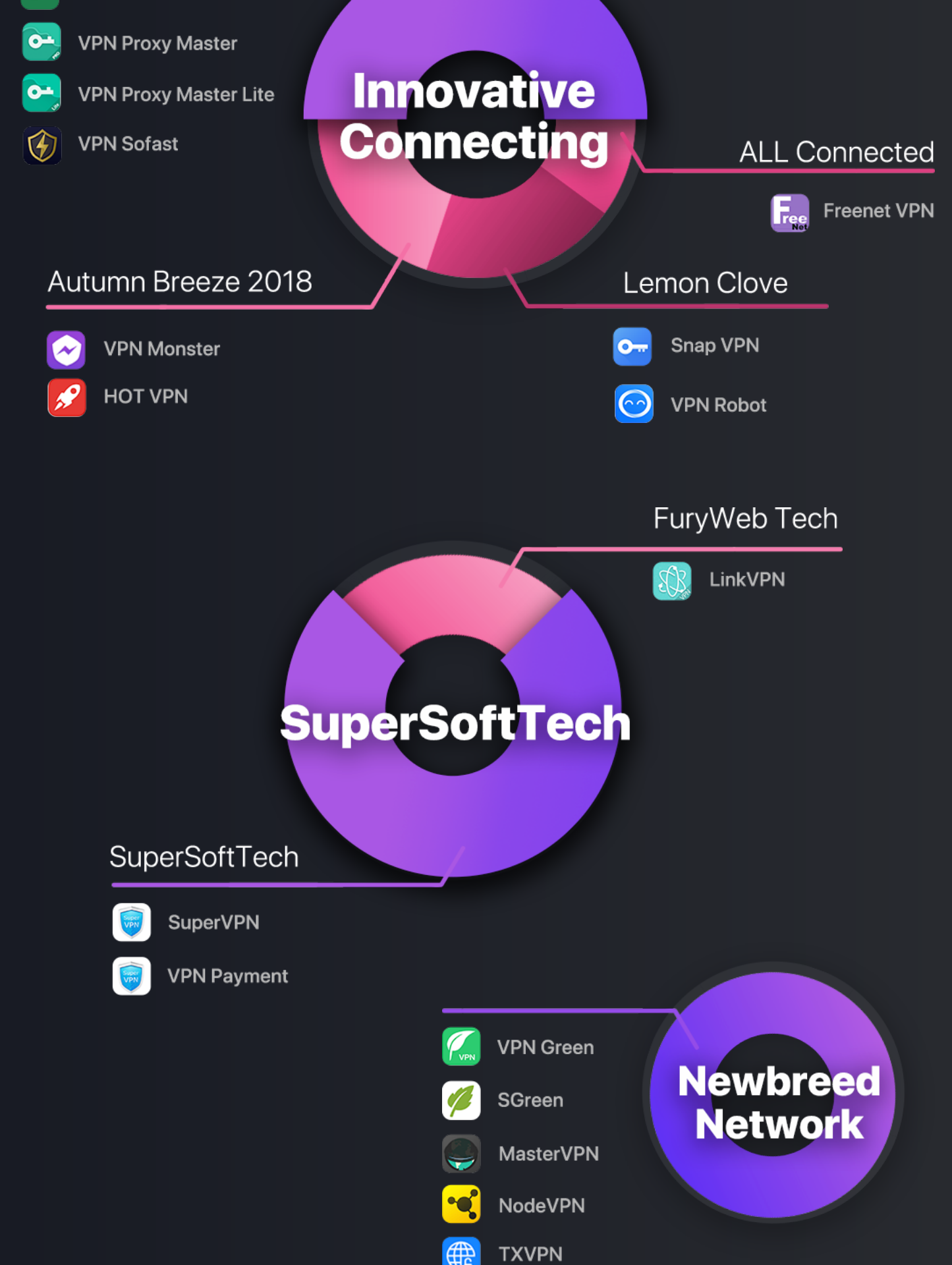


# The few behind the many: hidden VPN owners unveiled

VPN products that appear to be separate are all actually run by the same handful of companies. Even more, they're based in locations that aren't always privacy-friendly. Our research showed that **at least 97 VPN products are run by just 23 parent companies.**



## VPN Parent Company Location

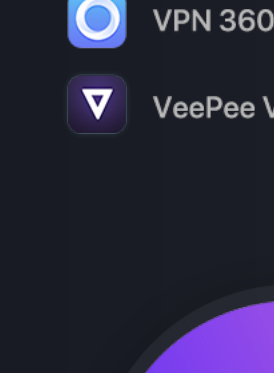
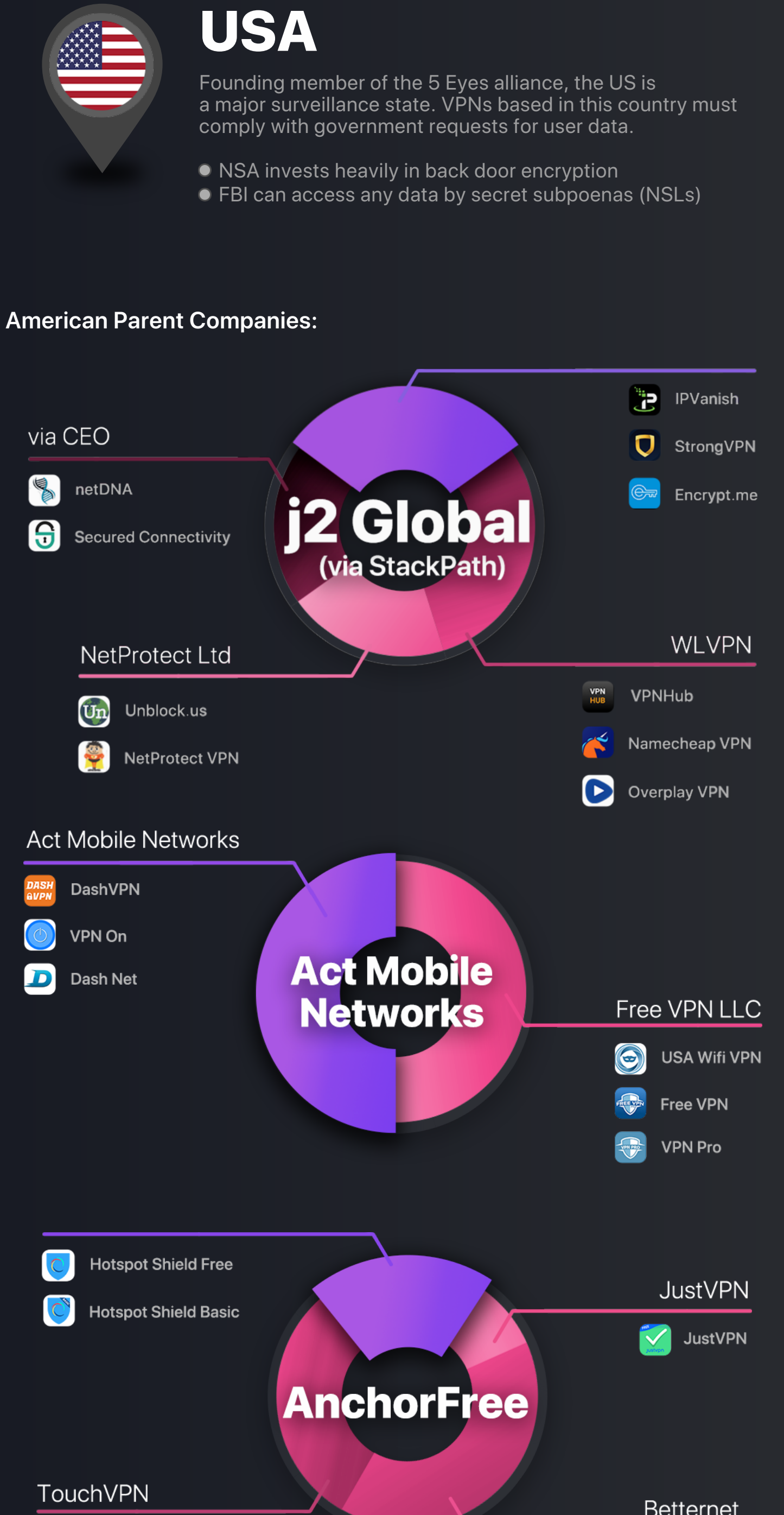


## China

One of the most repressive, surveillance-hungry nations with strict data retention laws. Having a VPN based in or connected to this country means your data is probably in the government's hands.

- China is a world leader in cyber spying
- Sponsors cyber attacks on foreign officials
- Government can ask for encryption keys, data, etc.

### Chinese Parent Companies:

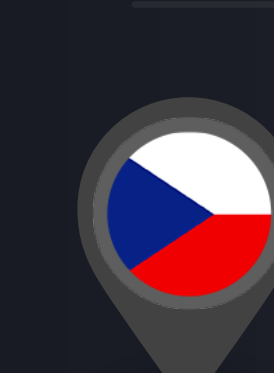
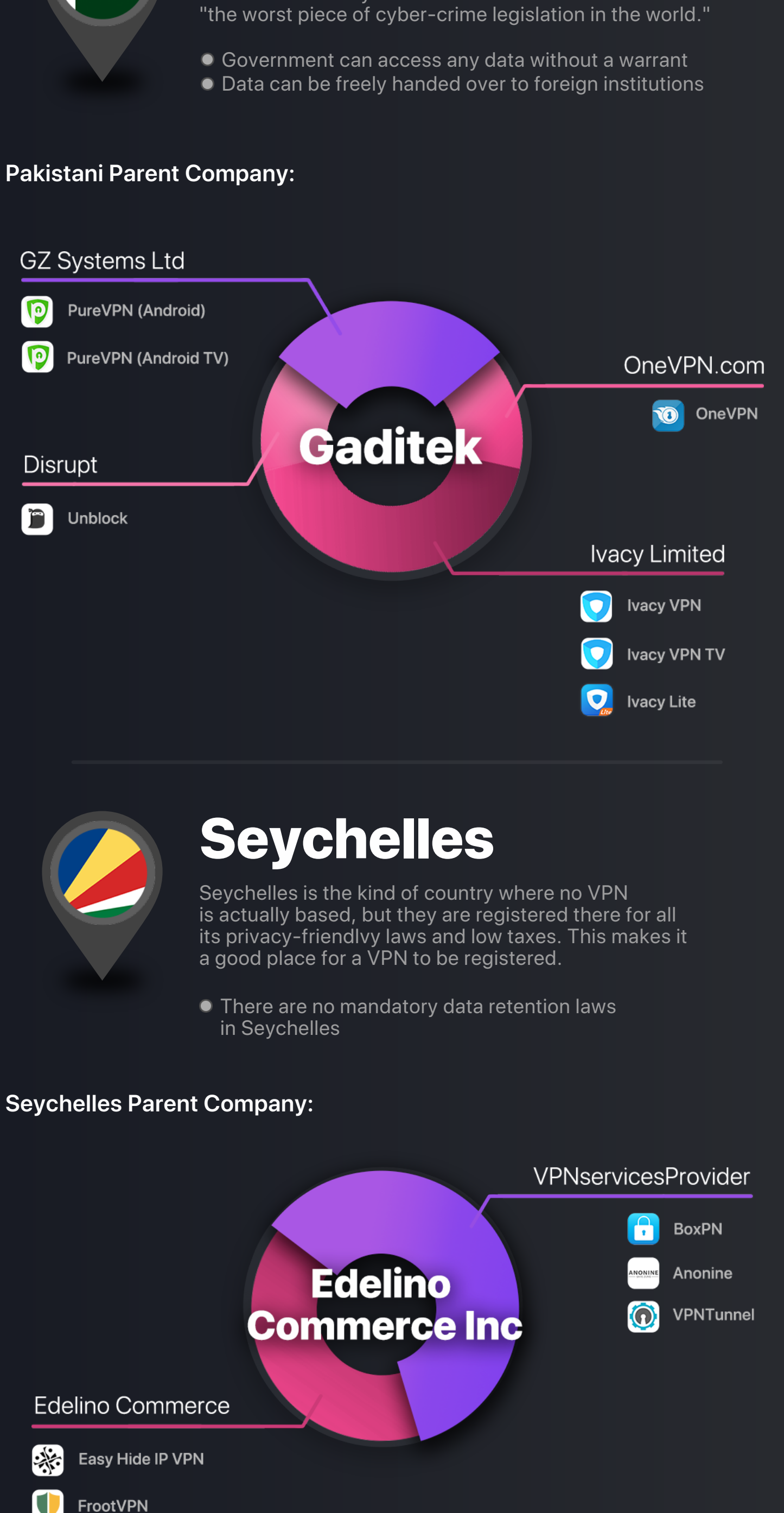


## USA

Founding member of the 5 Eyes alliance, the US is a major surveillance state. VPNs based in this country must comply with government requests for user data.

- NSA invests heavily in back door encryption
- FBI can access any data by secret subpoenas (NSLs)

### American Parent Companies:



## Pakistan

Pakistan's 2016 cyber-crime law has been called "the worst piece of cyber-crime legislation in the world."

- Government can access any data without a warrant
- Data can be freely handed over to foreign institutions

### Pakistani Parent Company:



## Seychelles

Seychelles is the kind of country where no VPN is actually based, but they are registered there for all its privacy-friendly laws and low taxes. This makes it a good place for a VPN to be registered.

- There are no mandatory data retention laws in Seychelles

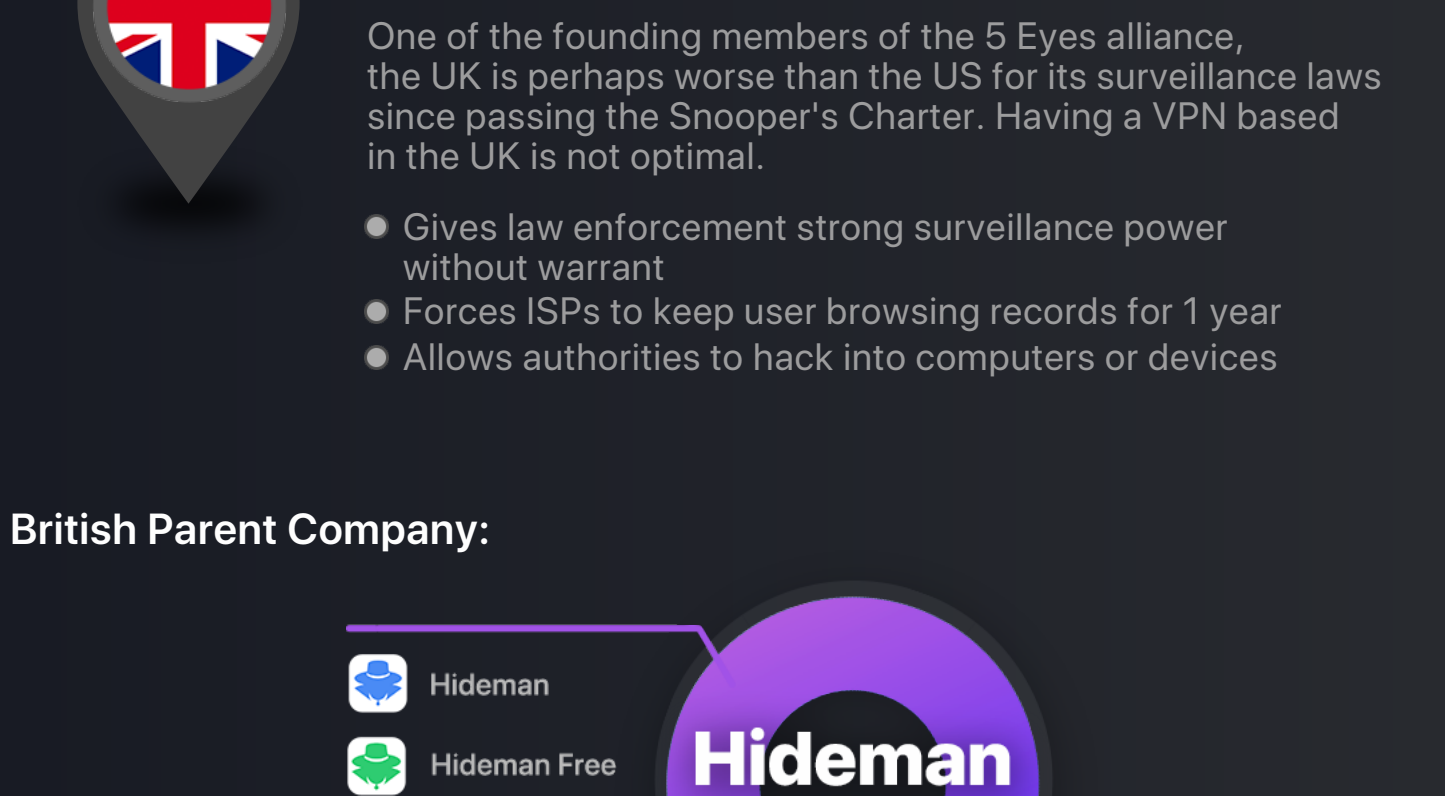
### Seychelles Parent Company:



## Czech

The Czech Republic is moderately safe when it comes to personal data protections. It is subject to the GDPR, which is enacted by all eurozone members, and has no mandatory data retention laws.

### Czech Parent Company:



## Netherlands

The Netherlands is a moderately safe country when it comes to personal data protections. It is subject to the GDPR, which is enacted by all eurozone members, and has no mandatory data retention laws.

### Dutch Parent Company:



## Isle of Man

Although not part of the EU, the Isle of Man has enacted data laws in line with the EU's GDPR. This makes it a good location to base a VPN.

### Isle of Man Parent Company:



## UAE

United Arab Emirates is a moderately safe country when it comes to personal data protections. There are no mandatory data retention laws in the UAE.

- VPNs are banned for "criminal" usage, with heavy fines or jail time

### UAE Parent Company:



## Hong Kong

Hong Kong is exempt from mainland China's laws and regulations. There are no mandatory data retention laws in Hong Kong. However, its proximity and relationship to mainland China is often worrying.

### Hong Kong Parent Company:



## UK

One of the founding members of the 5 Eyes alliance, the UK is perhaps worse than the US for its surveillance laws since passing the Snooper's Charter. Having a VPN based in the UK is not optimal.

- Gives law enforcement strong surveillance power without warrant
- Forces ISPs to keep user browsing records for 1 year
- Allows authorities to hack into computers or devices

### British Parent Company:



## Unknown

These VPN parent companies have no clear information about where they are based. It is very rare for VPN companies to not provide information about their company location. Since they could be based anywhere – including the UK, China, Russia, or worse – this is not optimal.

### Unknown Parent Companies:



Presented by: