Edward Snowden [US citizen in hiding in Russia], **Julian Assange** [Australian citizen holed up in the Ecuadorian Embassy in London], **Oliver Schmidt** [German citizen involved in Dieselgate, arrested on vacation in Florida and jailed for 7 years] all know that if US law enforcement wants to pursue you, there is very little you can do to hide.

Even though we are now in the era of FOSTA and the Cloud Act, realistically, individual providers are probably no more at risk from being individually targeted than they were before. The risks lie in becoming collateral damage in actions against other much larger targets, and having services upon which you rely withdrawn without notice, with a disastrous impact on your business.

“You don’t have to run faster than the bear to get away. You just have to run faster than the person next to you.”

Don’t be the low-hanging fruit - If law enforcement are looking for someone to subpoena in a case against an escort directory or a forum, make it a little tougher to determine your true identity and your activities. Realize that if you introduce a few more hurdles, they will likely move on from you to looking for an easier target.

.

Insure against the termination of vital services - Threats from government, or more likely from inhouse attorneys, can cause a hosting service, a cloud computing delivery network, or a website design service to decide they can do without the business of providers, and to terminate your service without notice. If such a service terminates your account, you will not be the only one affected and possibly hundreds of other providers will be looking for an urgent solution - the pressure of numbers will cause delays, running into weeks if not months. You have to ask yourself if you can afford that downtime. Have a fallback in place and ready to launch. Or better still, move now to a host, or a design house which is not going to leave you open to termination without warning or compensation.

“Hope for the best; plan for the worst.”

If you had your website created for you, the designers will probably have set up everything. So you may have no idea what privacy protection, if any, was established as part of that process.

If you want to have a little more detail, read on! But if you would simply like to **ask us to review your publicly available information and give you our informed (but not legal) opinion at no cost**, please respond to this email with you website URL (eg mydomainname.com).

You're reading on, so you'd like to know a little more. If you want to stay one step ahead of the curve, you need to consider each element of your web presence separately:

- Email
- Domain registration & privacy
- Hosting
- Website content

Email

Protonmail.com is fast becoming the goto standard for encrypted emailing. A basic account is free and operates just like Gmail,except your messages remain protected, especially if the person with whom you are corresponding has Protonmail as well. We suggest you get an account now. Our own email address is StickySites@ProtonMail.com

Domain registration & privacy

Your domain name is how you are known on the internet (eg mydomainname.com). It's your address. Your domain registrar and information can be checked here: https://whois.icann.org/en
The contact names and addresses should all be privacy-protected. If the name registrar or the privacy location are within the USA, you should consider moving your domain and privacy provider offshore. There is evidence that US-based privacy providers may give in to even gentle legal threats and reveal your information without notifying you in advance. Moving offshore doesn't guarantee privacy, but it's one more big investment of time and energy for anyone wanting to know your personal details. The best location to which to transfer your domain is complex and much-debated. You can choose to stick with your current name extension (.com) or create a new one not controlled in the USA (such as .at or .ch or .me). If you have owned your domain for a long time, it may be best to switch to a new extension as there are services which can report on all past domain name alterations, including any slip, however brief, that may have revealed your personal information. This decision will most likely be based on how much time, energy, and funds you think it justified to invest.
'Hope for the best, prepare for the worst'

Hosting

Your hosting service provides the location where your site is made available to view. It's your storefront. You can find out where you are hosted here: https://www.bitcatcha.com/.
Your website is probably hosted with one of a dozen major hosting companies, most of whom are US corporations based in the USA. Their Terms of Service vary, but a common theme, even if adult sites are not specifically forbidden, is that you may not conduct any illegal activity or do anything to bring the hosting corporation into disrepute. Recently Cloudflare terminated access by a twitter style forum with 50,000 members, without notice. Their site went down and it took a team of experts to find an alternative. It's worth noting that the only other time Cloudflare has banned a site was for a far-right organization in 2017.
If your site is hosted in the USA, or even by a US corporation who say they use offshore computer servers, you are at risk of termination without notice if they change their interpretation of their Terms of Service. So at the very least, keep a backup of your site somewhere else. If

you are with one of the self-design services like Wix or Squarespace, who do not allow you to backup and transfer your site anywhere else, then if they ban your class of site, you and many hundreds of others will have to start to build a site again from scratch at a time of crisis for all.
‘Hope for the best, prepare for the worst’

Website content
Unless and until cases are brought under the FOSTA legislation, it’s difficult to be precise on what should be excluded from a website in case it ‘facilitates prostitution’. Areas to consider include:

- Rates page, especially if it includes reference to working with another provider
- Client vetting requirements involving sites used by escorts or requesting other provider references
- FAQ’s setting out activities which are clearly sexual in nature
- Standard ‘time and companionship only’ warning which may be regarded as a clear indicator of the true nature of the site
- Inclusion of links to escort directories or vetting services (P411 has recently stated they still require a link on the front page but are safe because they are in Canada. They may be safe, but you are in the USA!)
- Touring information which is also a marker for an escort website

None of this is clear and you must make a decision on which aspects you are prepared to alter and where you are willing to take a small risk. Even if you make changes now, there are services which can provide snapshots of your web pages going back a decade, and FOSTA (though probably unconstitutionally) allows for prosecution in respect of actions you took before FOSTA was signed into law.

Overseas
FOSTA allows for the prosecution of anyone anywhere under the new regulations. It’s an affirmative defence if you can show that the activities in which you are engaged are legal in your jurisdiction. But that responsibility is on you. Remember the VW exec we mentioned at the start - he was a German citizen on vacation in Florida, but he had been found guilty of a crime in the USA, was arrested by the FBI, and now he’s in prison for 7 years…
There is also anecdotal evidence that proof of identity documents seized in raids on directory services, are being used to identify foreign providers and deny them entry on arrival in the USA.
‘Hope for the best; prepare for the worst’

In summary, and in most cases, our advice is:

Protect your privacy:

- Get a secure email account such as ProtonMail
- Move your domain offshore; consider starting afresh with a new domain extension such as .ch
- Move your hosting to a non-US corporation, using non-us servers, located in a country where prostitution is not illegal; do not rely on the hosting company marketing - independently check all these aspects
- Do not allow your host to use a cloud-based delivery service to speed your site (a CDN) as most are US owned and permit retention of any information passing through their servers

Secure against termination of your website services (taking down your site):

- Create a copy of your current website and install under a fresh domain and host selected as above; then if you are terminated, you can redirect traffic to the copy location within a few hours
- At the very least keep backups of your current website off your hosting servers
- If you are with a self-design host such as Wix or Squarespace, you cannot keep a backup and you should create a new website to your own preferred design (Wix & Squarespace prohibit copying their look) and install outside the USA

In closing, it's worth stating that much of the current alarm comes from an absence of informed comment or any indication of how vigorously this new law will be applied. The little comment to date suggests that targeting of individual providers is not the aim. Instead the target is the services offering the means of advertising, communicating, and operating your business.