6 Ways to Defend Your Privacy at the Border

By Dann Albright

Read the original article here: http://www.makeuseof.com/tag/border-privacy-passwords/

U.S. Homeland Security Secretary John Kelly has many privacy advocates worried. He recently testified that U.S. border agents could soon be asking visitors, “What sites do you visit? Oh, and give us your passwords.” This triggered a whirlwind of conjecture, condemnation, and confusion.

At the moment, **Kelly told NPR**, the Trump administration is considering demanding lists of websites, passwords, and social media accounts from people entering the U.S. from seven Middle Eastern countries. Also under consideration are searches of financial information and phone contacts.

This entire issue is a very thorny one. Is this type of search legal? Is it likely to start happening? And what can you do about it?

A Questionably Legal Search

The Fourth Amendment prevents the U.S. government from conducting "**unreasonable searches and seizures**." And requesting someone's password for their social media accounts seems very unreasonable. But this prohibition isn't enforced — at least not strictly — at the national border. Immigration agents have extended powers at the border and up to 100 miles from it.

But the issue is complicated, especially with digital information. As Orrin Kerr **pointed out to *The Atlantic***, a search of an online account could be considered to happen where the data is stored, and not at the border. This complicates the issue.

Because this practice hasn't actually been instated, there haven't been any significant legal challenges to it, further muddying the waters around its legality. The Department of Homeland Security does already ask people for their social media handles at the border. That in itself is quite controversial, despite it being optional. But there's no legal precedent for this type of search.

In short, the legality is very questionable. Especially with the Fourth Amendment already being essentially suspended at the border.

Will It Start Happening?

Of course, this is a very difficult question to answer. No one knows if the practice will be instated. There are, however, reports that some border agents have already started asking for passwords. It's certainly not unheard of in other countries that have a reputation for very tight border security. And the battle over getting access to personal devices has **already started in other quarters**.

With the attempted travel ban on people coming from predominantly Muslim countries, it seems likely that the current administration will at least try to put this practice into place. Whether or not they'll be successful, and whether asking for passwords would survive a legal challenge, is unknown.

Unfortunately, however, there's already a chance that travelers will meet this request when they try to enter the U.S., which means if you're planning on traveling there you should be prepared.

What Can You Do?

A number of experts have weighed in on what you should do to protect your **privacy** at the border. But because there's no legal precedent, which strategies will work, and which will get you denied entry, are also unclear. How far you're willing to go may depend on just how badly you need to get into the country, and what level of privacy you're willing to demand. **Just know that there is a chance you could be denied entry into the U.S.** Whether it's a significant chance or a small one — stop me if you've heard this one — is unknown.

Image Credit: Irina Gor via Shutterstock

We'll list these privacy-maintaining tactics in order from least drastic to most. The ones earlier in the list are easy, but probably less likely to work. The later ideas are more likely to work, but involve either significant effort or a good chance at being denied entry.

Note: We're not lawyers. And we certainly can't vouch for the legality of obfuscating your account information. The laws differ around the world, as do the consequences of violating them. Use your head, don't do anything stupid, and know the laws of where you're traveling.

1. Delete Your Social Media and Email Apps

This is rather simple, but it's also only likely to work if you don't have mobile data on your phone. If you do, there's a chance you'll be directed to re-download the apps and sign in. If you don't, though, it's possible that the hassle of getting your phone on the airport Wi-Fi (if there is any to speak of) and asking you to sign in via your mobile browser will dissuade a border agent from getting too curious.

2. Enable Two-Factor Authentication

This is **something you should do** anyway. But if you're concerned about your **privacy** at the border, you'll need to take some additional steps. You'll have to sign out of your accounts to make sure the 2FA gets triggered, for example. And you'll also have to not have any of your other devices with you. That way there's nothing you can do should an agent demand you sign into your accounts with the 2FA code.

How will you get back into your accounts once you're past the border? You'll need to have someone tell you the 2FA code (you could give a backup code to someone you trust and can call later) or mail one of the devices that can unlock your accounts to the address you'll be staying at. It's a hassle, but it works.

3. Use a Burner Device

We've talked about how burners can **help protect your privacy** before. And when you're traveling internationally, it makes sense to carry one anyway. If your primary phone **gets stolen**, there's a ton of sensitive data on there that could be at risk. Carrying a cheap burner that doesn't have access to your accounts means you can't access them at the border. If you need your actual device, again, you could mail it to yourself. You could also buy a new one upon entry.

Both of these choices will be a pain, but they'll protect your privacy without having to give up all forms of communication while you travel.

4. Use a Different Email Account for Social Accounts

When combined with effective two-factor authentication, a second email address that isn't synced to your phone will prevent a border agent from resetting your passwords and then accessing your accounts. If you're okay with a border agent looking through your primary email account, this will work. It will also keep them from accessing your social accounts. Just make sure to not have any trace of this secondary account on your device.

5. Switch From Fingerprints to Passcode

If you currently use your fingerprint to unlock your phone, consider **changing to a passcode**. At least in the United States, you can be legally compelled to unlock a phone with your print. But you can't be compelled to enter your code (at least for now). You can reasonably refuse a request to unlock your phone with a passcode at the time of this writing, which leads us to the final option…

6. Refuse

As you might expect, this is not going to go over well. In the United States, it's almost certainly legal. But that doesn't mean it's a good idea. There's probably a very good chance that you'll be denied entry. That applies regardless of where you're coming from, where you're a citizen, and what your business in the country is. This is an absolute last resort, and probably not one to use if you're just sticking up for your rights.

A Few More Notes

There are a couple other things to keep in mind. Shipping your devices overseas, for example, doesn't mean that they'll be immune to search. International delivery of your devices is a good option if you don't want your device with you at the border. But packages being sent across borders are also subject to scrutiny.

And this should probably go without saying, but try to not make a huge deal out of the situation if you get stopped or asked for your passwords. The more you can fall back on things you *can't* do instead of things you *won't* do, the less likely you'll be to irritate the border agent. Which is good for everyone.

It's worth repeating: none of this is legal advice. And with how quickly laws and regulations are changing in the U.S. right now, any of this may become illegal or irrelevant by the time you read it. Check for information from organizations like the **American Civil Liberties Union**, the **Electronic Freedom Foundation**, and **Privacy SOS** before you travel.

Are you nervous about your **privacy** at the U.S. border? Have you been asked for this information? Or do you think the collection of social media and website passwords is warranted? Share your thoughts **in the comments**!

Image Credits: 1000 Words/Shutterstock