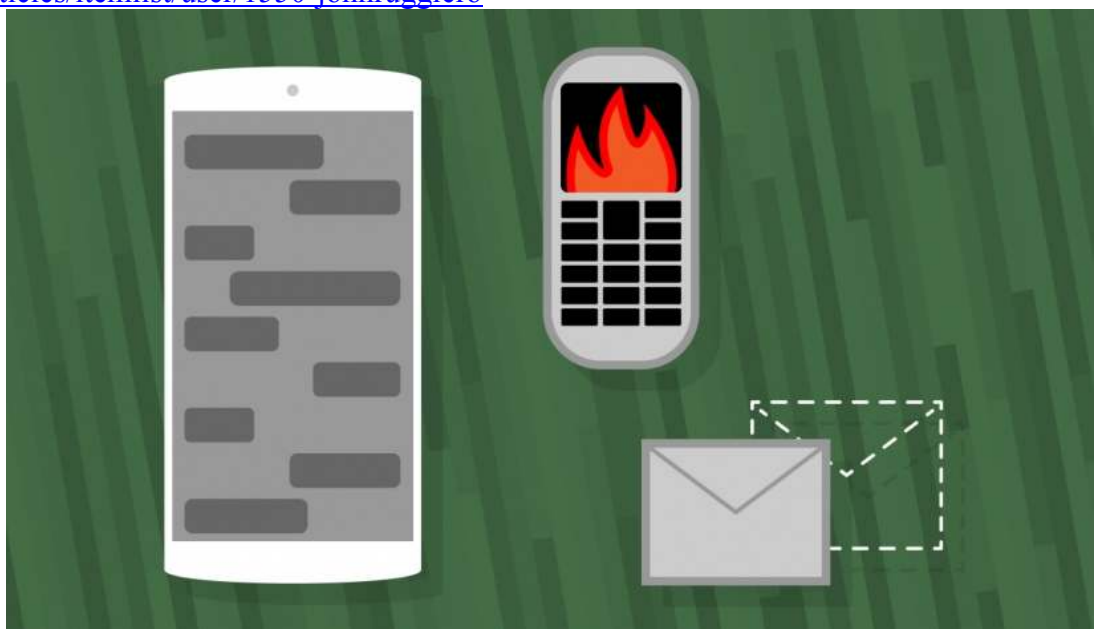
SOURCE: https://www.airsassociation.org/services-new/airs-knowledge-network-n/airs-articles/item/16855-tech-tips-to-help-stay-safe-in-trump-s-america?utm_content=buffer0b73e&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer

Tech tips to help stay safe in America

Posted by John Ruggiero
https://www.airsassociation.org/services-new/airs-knowledge-network-n/airs-articles/itemlist/user/1550-johnruggiero



Tech is as much a liability as it is an opportunity, as this election demonstrated. The next few years will be scary for many reasons, and to some more than others, and part of that will be the continued and likely expanded exploitation of the technologies and services we've come to rely on. Communities likely to be targeted by the 45th President policies may want to take a few steps online to help ensure their safety and privacy.

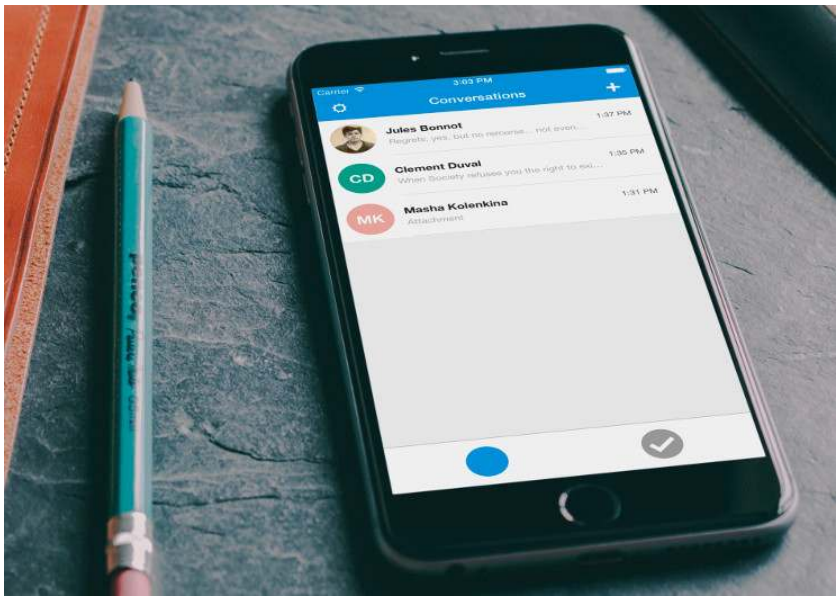
The 45th President has gone on the record asking for backdoors to encryption and devices, saying he supports surveillance, and is against Net Neutrality. Policies pursuant to these goals will necessarily put your data at risk.

The following are privacy tips anyone can use, but they are particularly relevant for anyone who, for example, plans to participate in protests or grassroots organizing, or for undocumented immigrants who would like to decrease their online presence. I've listed them roughly in order of importance.

Ditch SMS and use end-to-end encryption

If the 45th President makes good on his promise to make deportation of undocumented immigrants, you can expect police to bring the same measures they use in serious crimes to bear on this task. One such measure is the interception of mobile phone calls and messages, whether using a Stingray-type device (which imitates a cell tower, causing phones to send it data instead) or more traditional tapping at the network level.

Ordinary phone calls and text messages are incredibly easy to collect this way, and are often also exposed as part of other investigations. It's easily imagined that the police may run a dragnet in areas densely populated by immigrants and watch for keywords pertaining to under the table employment, family across the border, remittances, and so on.



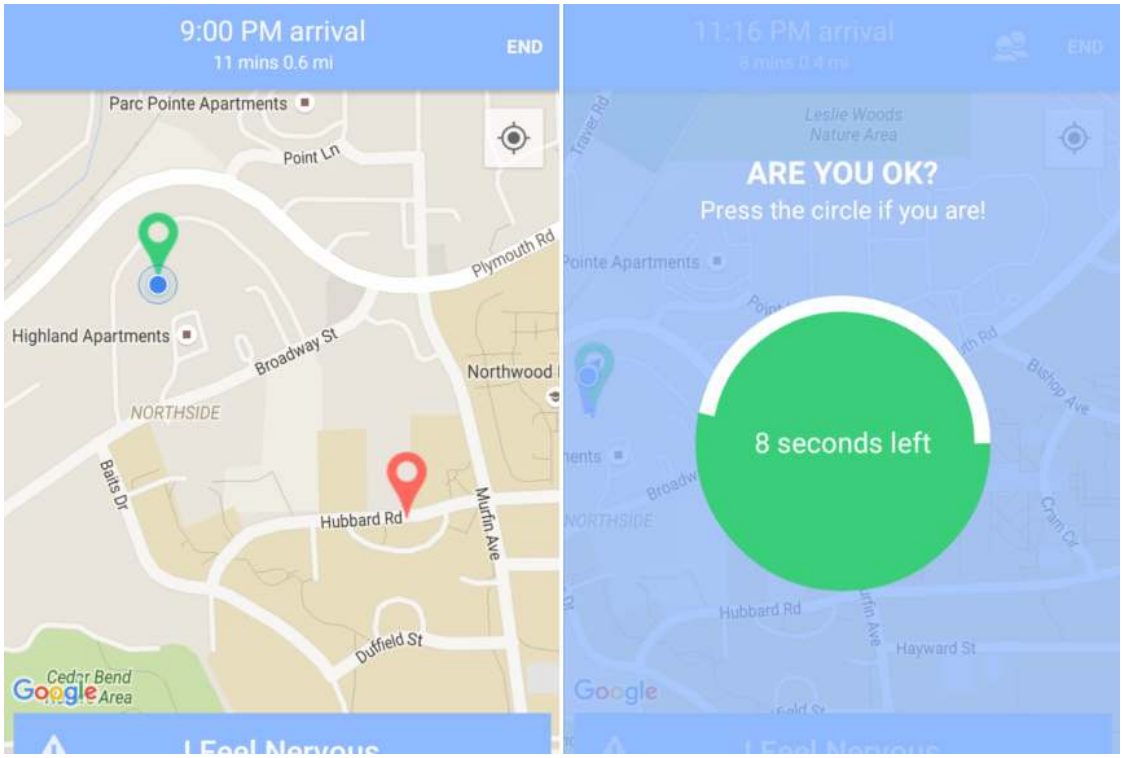
They can't do that if you're using an app like Signal https://whispersystems.org/, which uses "end-to-end encryption," preventing electronic snooping anywhere along the line — including on the service's own servers and while the data is in transit between networks and devices. This type of encryption is the bane of every authority because not only can they not see what is being sent, nor can the company that runs it, so the information can't be subpoenaed or hacked out.

It may be a pain, but getting your family and friends switched over to one of these apps could prevent a lot of trouble down the line.

Some other options, if for some reason Signal doesn't work: WhatsApp is a popular and versatile option, but it's owned by Facebook, and while it's technically independent, that still makes us nervous. Apple's iMessage is reliable and popular, but requires an iOS device or Mac — Apple is also under tremendous scrutiny, having been called out specifically by the 45th President as a company to put pressure on.

Avoid Allo and Telegram, which have been criticized for their encryption and privacy choices.

Use a get-home-safe app



The 45th President's naked xenophobia, tacit support of vigilantism, and lack of concern over police militarization and brutality suggest it may soon become far less safe for people of color, Muslims and Sikhs, LGBT individuals and other targeted minorities to walk home alone. Tech can't prevent bigotry and bashing, but it can at the very least help create a safety net.

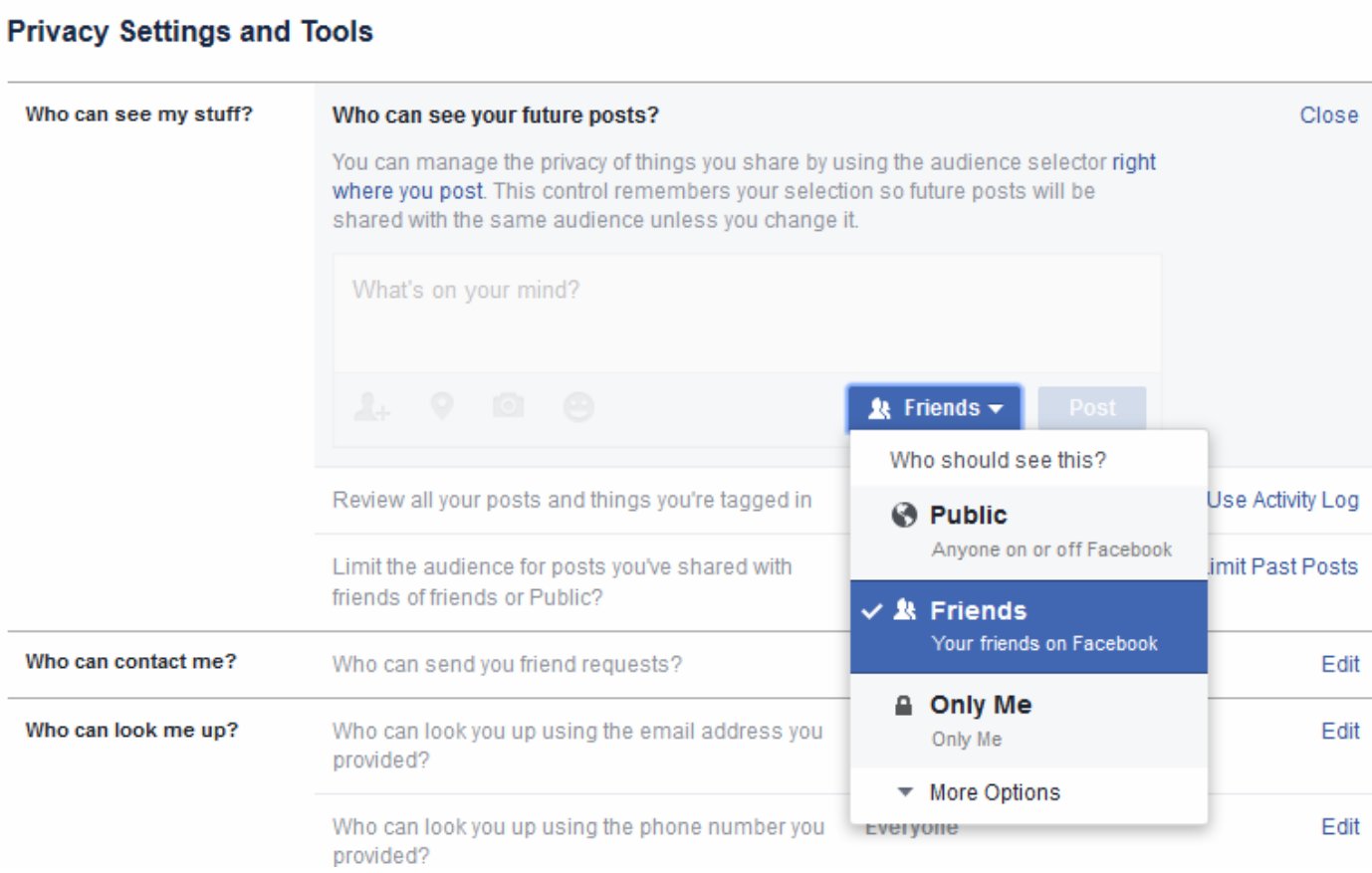
Apps like Kitestring https://www.kitestring.io/ and http://www.companionapp.io/ Companion let you set emergency contacts, and if you, for example, don't check in at home within 15 minutes, or if you shake the phone hard for 5 seconds, it will send them your location and a message that you need help. (They use SMS, but we'll make an exception in this case.)

It's scary and unfair that this should even have to be recommended, but it's an opportunity to protect yourself using technology you already have. Check with some friends and see what app looks best.

Go private on Twitter, Facebook, Instagram, and Google

Part of the fun of social networks is the idea that you're sharing with the world. But law enforcement also uses them as investigative tools, establishing whereabouts, work

history, and anything else that your posts imply. Like anything you say to the police, this can and will be used against you, and if you have reason to think you may be targeted by them, you should make it difficult to get at. Making your account private is an easy way to do that, even if it'll be harder to garner followers.



Be sure to check your preferences and privacy settings in every app and service and opt out of things like default public check-ins or anything with "personalized," "tailored," or "curated" in it — it means they're reading your data.

On Google, you should turn off ("pause") your location history https://myaccount.google.com/activitycontrols/location and opt out of other tracking measures in the search https://www.google.com/preferences and ads https://www.google.com/settings/ads areas. On your phone, you can turn off location services or restrict them per app. Using an alternative to Google, like DuckDuckGo https://duckduckgo.com/, helps keep your browsing habits private.

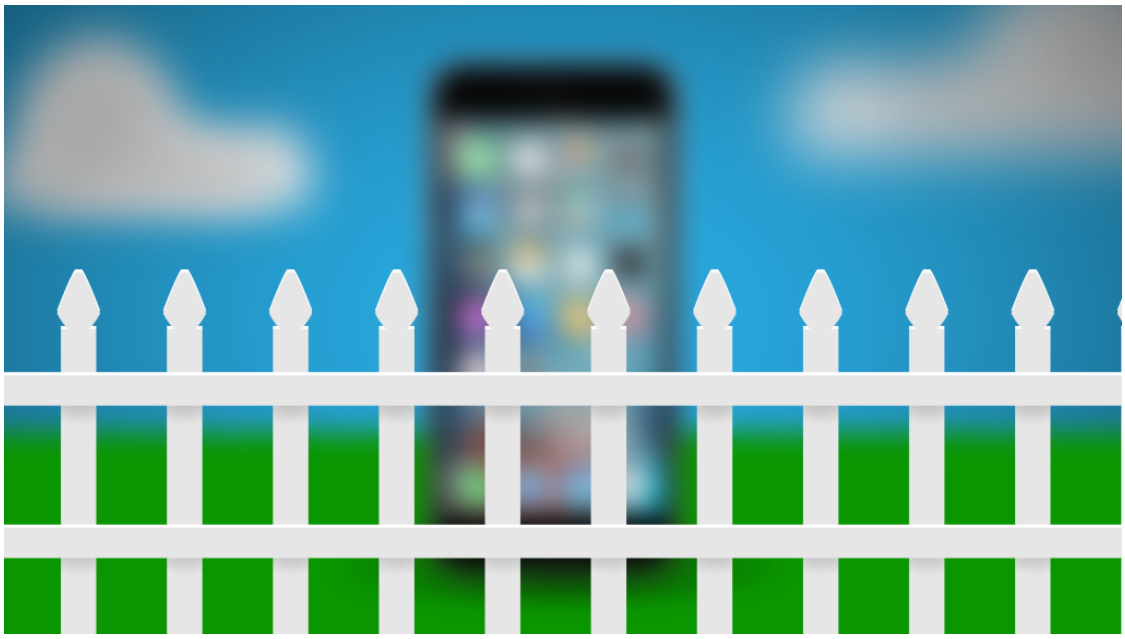
Install HTTPS everywhere

The Electronic Frontier Foundation has a plug-in https://www.eff.org/https-everywhere for Chrome, Firefox, and other browsers that forces them to make a secure connection even when it isn't the default for the website or service you're connecting to. You'll also

be warned when the connection isn't secure (browsers also tell you this, but not very loudly).

Keep your phone and PC software up to date

The latest versions of Windows, macOS, Android, and iOS don't bring just the latest features, but also lots of fixes for serious security holes. These fixes will apply to a few of the previous versions, but not really old ones. Hackers — and the authorities — know this. If your phone and OS are new enough to take full advantage of encryption tools and resist well-known methods for unlocking and hacking, they're secure against adversaries domestic and foreign.



It isn't always easy to stay updated, but keep it in mind when buying a new phone or computer. If you're on an OS more than a year or two old — before things like full-disk encryption were standard — you should consider updating at the earliest opportunity.

Slightly older iPhones will still get the critical updates (mainly iOS 8) that added broader encryption, as will Nexus phones and other flagship devices. Budget (but still modern) phones like the Moto E and G are also great options for those on a budget.

Look into a VPN

Virtual Private Networks obscure your internet traffic from your ISP and others by routing it through other servers first. If all your connections are to your VPN (which then passes it on to wherever it was headed), and your VPN doesn't keep any records of those connections, there are far fewer ways for your browsing to be tracked.

Good VPNs cost money. We don't recommend any VPN in particular, but it should be a VPN that plainly states that it doesn't log your traffic. Examples include ExpressVPN https://www.expressvpn.com/, Anonymizer https://www.anonymizer.com/, and Private Internet Access https://www.privateinternetaccess.com/. There are dozens to choose from, however, and I don't claim to be an expert; many are reviewed https://thatoneprivacysite.net/ here if you want to be careful about the jurisdiction the VPN is based, the extent of its record keeping, and so on.

Get a backup/burner phone

If you attend lots of protests or demonstrations, or often choose to film police encounters, you might want to keep a burner phone around in case yours gets smashed or confiscated. You can get a cheap Android phone for $100 or less, and if you aren't relying on SMS and phonecalls, you can do pretty much everything you need over wi-fi until you get a replacement.

Change your DNS

Should the authorities choose to enforce blocks of certain websites — for your own sake, of course — the easiest way to do it is ordering major domain name services (which connect URLs like techcrunch.com to IP addresses like 155.91.18.66) to simply prevent internet users from getting to them. Fortunately, this type of censorship is as easy to circumvent as it is to put in place.

You can easily change the DNS your computer uses in its network settings. OpenNIC has detailed instructions https://www.opennicproject.org/configure-your-dns/ for various operating systems, and has proven itself trustworthy. Google's Public DNS https://developers.google.com/speed/public-dns/ is another option, and has the benefit of being easy to remember: change the preferred and alternate DNS servers to 8.8.8.8 and 8.8.4.4 respectively.

Set up Firechat or another offline communication tool

Another way governments have quashed dissent is by suppressing mobile communication altogether. It can't hurt to have an app like Firechat http://www.opengarden.com/firechat.html installed on your phone, which passes messages directly between devices without the need for a network. This is also useful in case of power outages and other disasters — a good emergency measure to take regardless.

Avoid the "Internet of Things"

Even if the various smart appliances worked well, we'd still have issues with their security and the way data is handled https://techcrunch.com/2016/02/01/harvard-report-debunks-claim-surveillance-is-going-dark/. You're not missing out on much, so just skip the wi-fi front door lock and Amazon Echo for now.

Go end-to-end encrypted on email and cloud storage too

This is harder to do for many people, since services like Gmail and Dropbox have become practically ubiquitous. But if you're really worried about privacy, there are options that provide similar services but with a "zero knowledge" guarantee — basically that the company that runs them never knows a thing about what you use their service for.

ProtonMail https://protonmail.com/ is a solid one if you're looking to get away from Gmail, or just have a second email for sensitive topics. SpiderOak One https://spideroak.com/solutions/spideroak-one is like a super-private Dropbox.

Install an alternative OS

If you're really worried about snooping, consider using an alternative to the standard operating systems that's designed with privacy and security in mind. This isn't an easy option but it might be good to explore if you have an old laptop or phone lying around.

Copperhead https://copperhead.co/android/ is worth trying if you're used to Android, although it won't have all the conveniences of the usual Google-powered version. Tails https://tails.boum.org/ is what Edward Snowden has recommended for desktop and laptop work that needs to stay private. It's basically a simple, security-focused OS that deletes itself when you're done.