The Intercept_

Micah Lee

February 20 2017, 9:53 a.m.

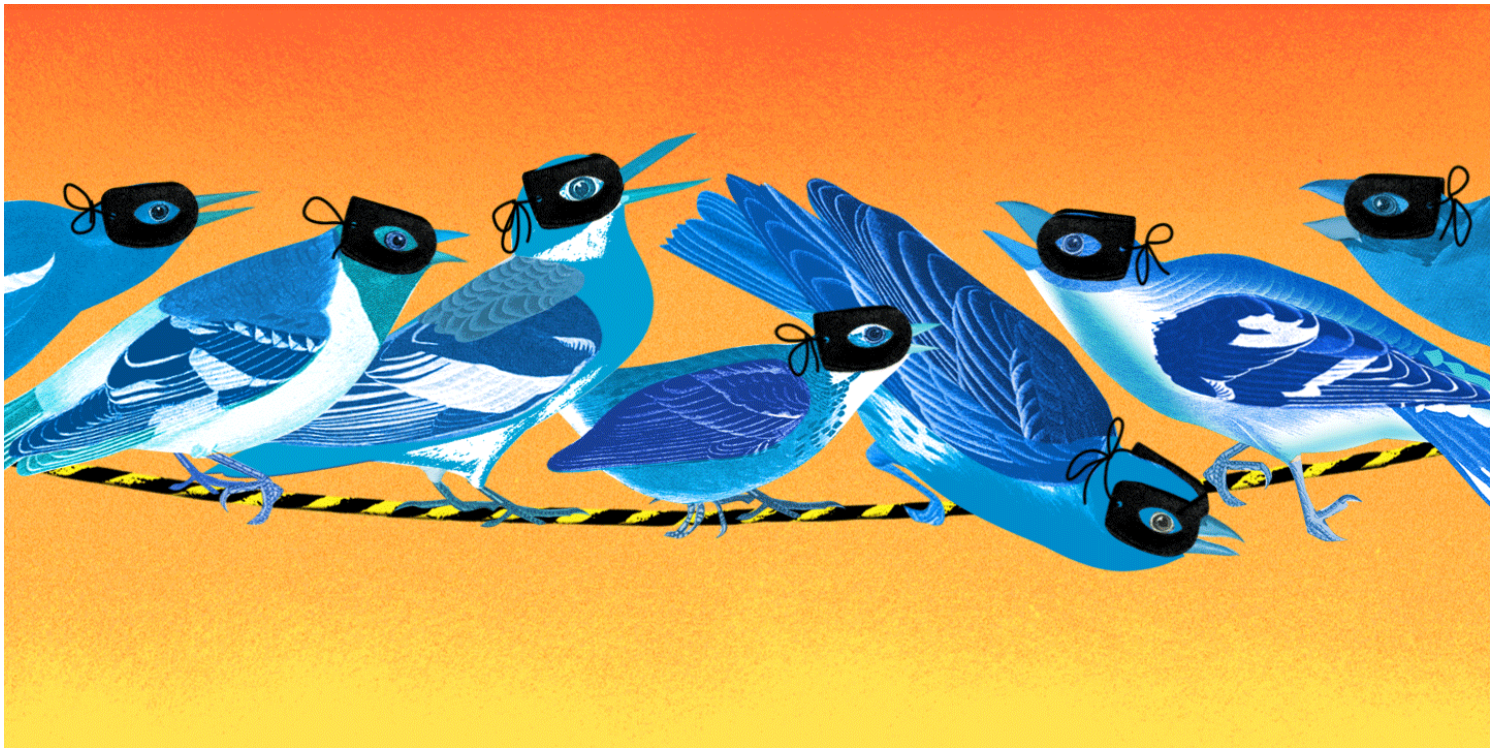


Illustration: Doug Chayka for The Intercept

LEIA EM PORTUGUÊS ⟶

One of the first things Donald Trump did when he took office was temporarily gag several federal agencies, forbidding them from tweeting.

In response, self-described government workers created a wave of rogue Twitter accounts that share real facts (not to be confused with "alternative facts," otherwise known as "lies") about climate change and science. As a rule, the people running these accounts chose to remain anonymous, fearing retaliation — but, depending on how they created and use their accounts, they are not necessarily anonymous to Twitter itself, or to anyone Twitter shares data with.

Anonymous speech is firmly protected by the First Amendment and the Supreme Court, and its history in the U.S. dates to the Federalist Papers, written in 1787 and 1788 under the pseudonym Publius by three of the founding fathers.

But the *technical* ability for people to remain anonymous on today's internet, where every scrap of data is meticulously tracked, is an entirely different issue. The FBI, a domestic intelligence agency that claims the power to spy on anyone based on suspicions that don't come close to probable cause, has a long, dark history of violating the rights of Americans. And now it reports directly to President Trump, who is a petty, revenge-obsessed authoritarian with utter disrespect for the courts and the rule of law.

In this environment, how easy is it to create and maintain a Twitter account while preserving your anonymity — even from Twitter and any law enforcement agency that may request its records? I tried to find out and documented all my steps. There are different ways to accomplish this. If you plan on following these steps, you should make sure you understand the purpose of them, in case you need to improvise. I also can't guarantee that these techniques will protect your anonymity — there are countless ways that things can go wrong, many of them social rather

than technical. But I hope you'll at least have a fighting chance at keeping your real identity private.

For this exercise, I decided to pick a highly controversial political topic: Facts. I believe that what we know about reality is based on evidence that can be objectively observed. Thus, I created the completely anonymous (until publishing this article, of course) Twitter account @FactsNotAlt. Here's how I did it.

Threat model

Before we begin, it helps to define a threat model, that is: what we need to protect; who we need to protect it from; what their capabilities are; and what countermeasures prevent or mitigate these threats.

Basically, it's impossible to be completely secure all the time, so we need to prioritize our limited resources into protecting what matters the most first. The most important piece of information you need to protect in this case is your real identity.

Law enforcement or the FBI might launch an investigation aimed at learning your identity. It may be to retaliate against you — getting you fired, charging you with crimes, or worse. Your Twitter account might also anger armies of trolls who could threaten you, abuse you with hate speech, and try to uncover your identity.

If the FBI opens an investigation aimed at de-anonymizing you, one of the first things they'll do is simply ask Twitter — and every other ser-

vice that they know you use — for information about your account. So a critically important countermeasure to take is to ensure that none of the information tied to your account — phone numbers, email addresses, or IP addresses you've used while logging into your account — lead back to you.

This is true for all accounts you create. For instance, if you supply a phone number while creating your Twitter account, the phone service provider associated with that number shouldn't have information that can lead back to you either.

Another concern: The FBI also might go undercover online and try to befriend you, to trick you into revealing details about yourself or to trick you into clicking a link to hack you. They might make use of informants in the community of people who follow you on Twitter as well. Organized trolls might use the same tactics.

Hiding your IP address with Tor

An IP address is a set of numbers that identifies a computer, or a network of computers, on the internet. Unless you take extra steps, every website you visit can see your IP address. If you're using Twitter while connected to your home or office Wi-Fi network, or your phone's data plan, Twitter can tell. If they hand these IP addresses to the FBI, you will very quickly lose your anonymity.

This is where Tor comes in. Tor is a decentralized network of servers that helps people bypass internet censorship, evade internet surveillance, and access websites anonymously. If you connect to Twitter while you're using Tor Browser, Twitter can't tell what your real IP address is — instead, they'll see the IP address of a random Tor server. Tor servers are run by volunteers. And even if any of the servers bouncing

your data around are malicious, they won't be able to learn both who you are and what you're doing.

This is the primary benefit that Tor has over Virtual Private Network, or VPN, services, which try to help users hide their IP addresses. The FBI *can* go to a VPN service to learn your real IP address (assuming the VPN keeps a record of its users' IP addresses and cooperates with these requests). This isn't true with Tor.

To get started with Tor, download Tor Browser. It's a web browser, like Chrome or Firefox, but all its internet traffic gets routed over the Tor network, hiding your real IP address.

Using Tor Browser is the easiest way to get started, but it's not perfect. For instance, a hacker who knows about a vulnerability in Tor Browser can discover your real IP address by tricking you into visiting a website they control and exploiting that vulnerability — the FBI has done this in the past. For this reason, it's important to *always* immediately update Tor Browser when you get prompted.

You can also protect yourself from Tor Browser security bugs by using an operating system that's designed to protect your anonymity, such as Tails or Qubes with Whonix, (I've written about the latter here). This is more work for you, but it might be worth it. Personally, I'm using Qubes with Whonix.

Getting an anonymous email address

Before you can create nearly any account online, you need an email address. While popular email services like Gmail or Yahoo Mail let anyone make an account for free, they don't make it easy to do so anonymously. Most of them require that you verify your identity with a phone number. You can in fact do that anonymously (more on that below), but I

prefer using an email provider that is happy to give addresses to anonymous users.

One of these providers is SIGAINT, a darknet-only service that forces all its users to log in using Tor to read or send email. The people who run it are anonymous and it contains ads for (sometimes very sketchy, sorry) darknet websites. However, you do end up with a working, anonymous email address.

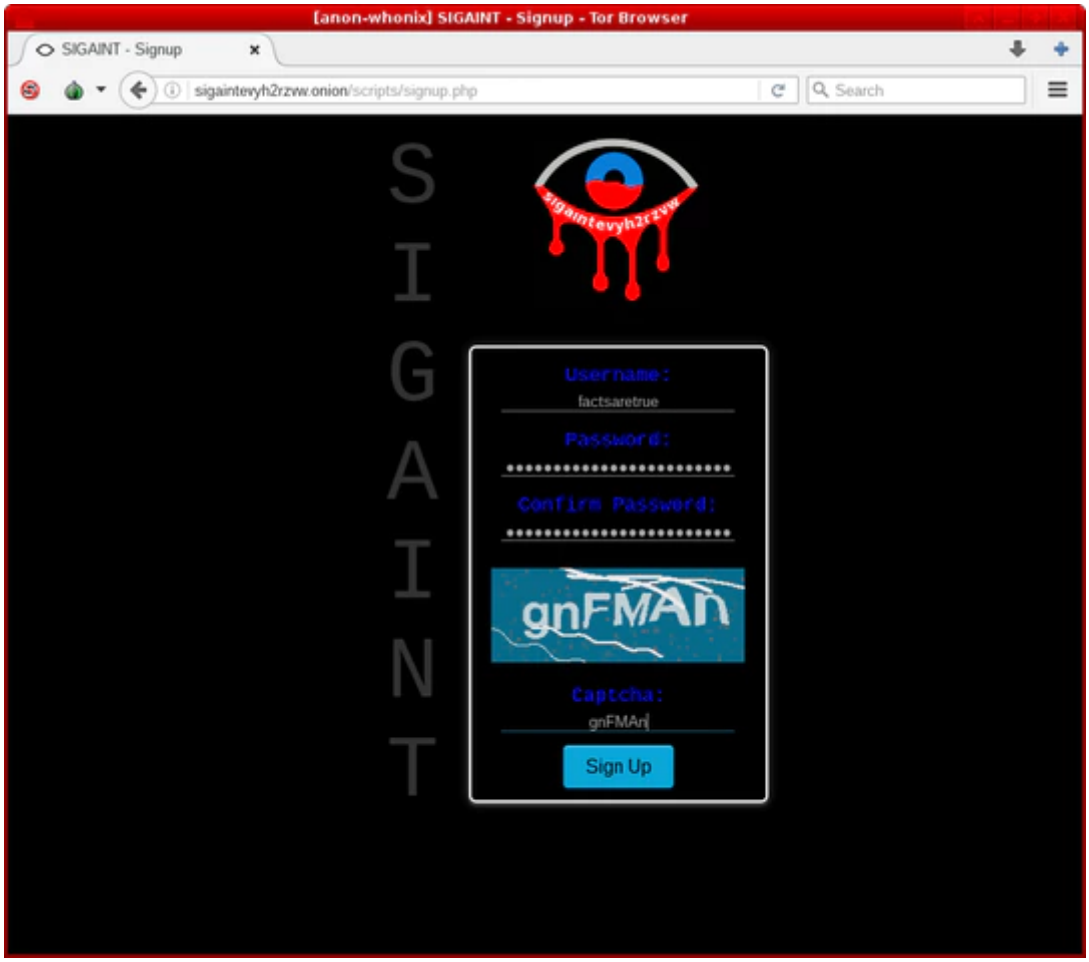
Update: Feb. 20, 3:10 p.m. ET
The SIGAINT service appears to be down right now. While it's down, you can try Riseup or set up a burner phone and then try ProtonMail, Gmail, or some other service instead.

If you prefer not to use SIGAINT, another good choice is Riseup, a technology collective that provides email, mailing list, VPN, and other similar services to activists around the world. Accounts are free, and they don't ask for any identifying information, but you do need an invite code from a friend who already uses Riseup in order to create an account.

Yet another option is ProtonMail — a privacy-friendly email provider based in Switzerland that asks for minimal identifying information and works well over Tor. However, to prevent abuse, they require Tor users to provide a phone number (that they promise not to store) to receive an SMS during account creation. So, if you'd like to use ProtonMail instead (or any other email service that requires a phone number when creating an account over Tor), follow the steps below to create an anonymous phone number first.

I decided to use SIGAINT. In Tor Browser, I went to SIGAINT's onion service address, sigaintevyh2rzvw.onion, which I found on their public website. This is a special type of web address that *only* works in Tor

Browser, and not the normal internet. From there, I filled out the form to create a new account.



That's it. I've now created a brand new anonymous email address: factsaretrue@sigaint.org.

Getting an anonymous phone number

While attempting to create a Twitter account, I quickly hit a snag. Even if I provide my (anonymous) email address, Twitter won't let me create a new account without first verifying my phone number. (You might get lucky and get the option to skip entering your phone number — it doesn't hurt to try — but if you're coming from a Tor node that isn't likely.)

This is a problem, because I obviously can't use my real phone number if I want to remain anonymous. So to proceed, I needed to figure out how to get a phone number that isn't tied to my actual identity. This is a common problem when trying to stay anonymous online, so you can follow these instructions any time you need a phone number when opening an account.

There are other ways to do it, but I chose a conceptually simple option: Buy a burner phone anonymously, use it to verify my new Twitter account, and then get rid of it. I wandered around downtown San Francisco looking in convenience stores and pharmacies until I found what I was looking for in a 7-Eleven.

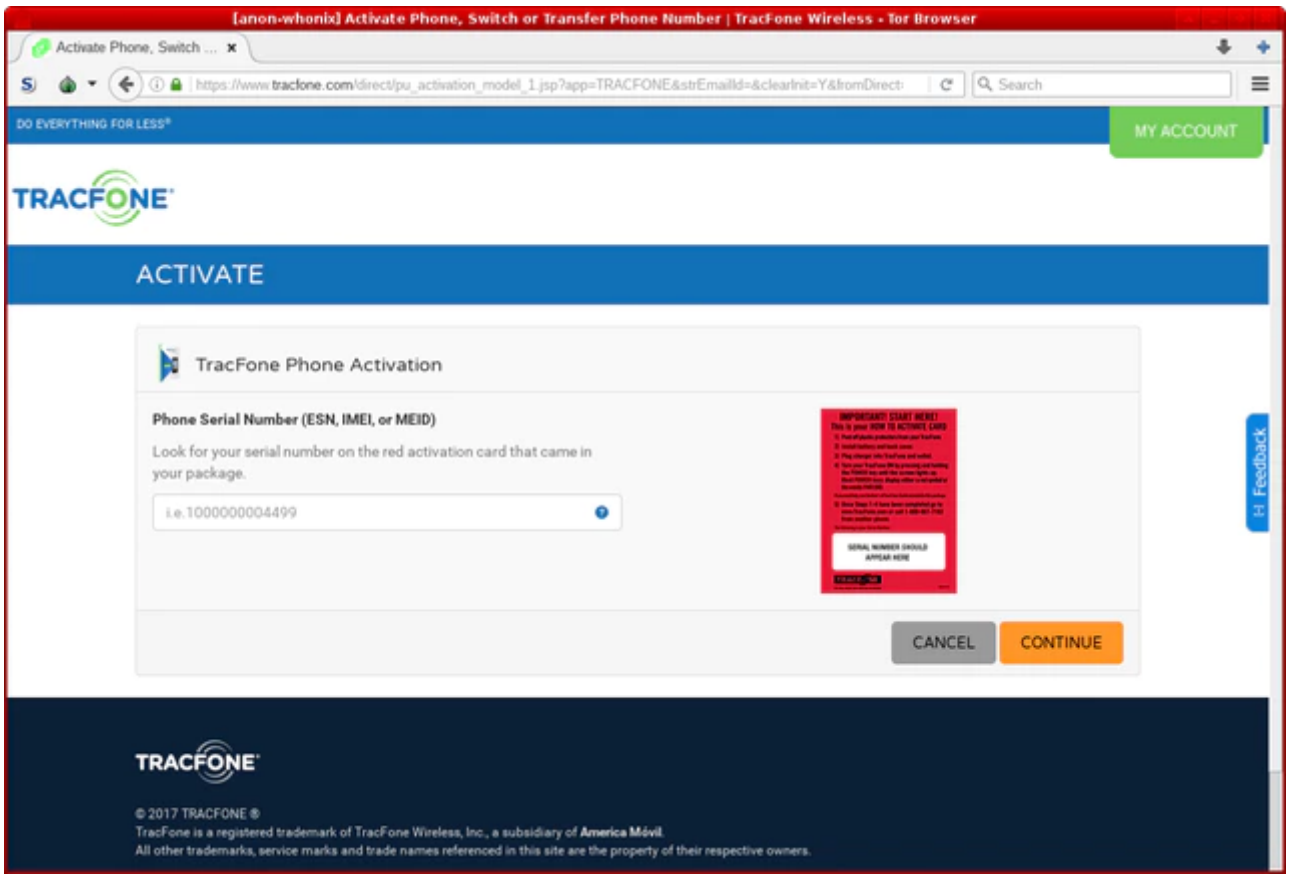
Using cash, I bought the cheapest TracFone handset I could find (an LG 328BG "feature phone" — as in, not a smartphone) as well as 60 minutes' worth of voice service, for a total of $62.38 after tax. You might be able to find cheaper cellphone handsets if you look long enough.

If you're going to get a burner phone and want to maintain your anonymity, here are some things to keep in mind:

- Buy your burner phone handset and pre-paid service using cash. Don't use a credit card.
- When you buy service, the clerk activates your service card at the cash register. This tells the phone company (TracFone, in my case) exactly which store you bought it from, and when. Keep this in mind and consider picking a store far away from where you live — like while you're traveling in another city.
- Security cameras will probably record your face at the store. Most stores delete old footage on a regular basis, overwriting it with new footage. If possible, wait a week or two before you start tweeting so that the footage is already deleted by the time anyone tries to figure out your real identity.
- You can find phones and service like this at some convenience stores and pharmacies. If you need to do internet research to find a store near you that sells burner phones, use Tor Browser.
- As soon as you power on your burner phone, it will connect to cellphone towers, and the phone company will know your location. So, don't activate your phone, or keep it powered on at all, at your home or office — instead, go to a public place, like a coffee shop, before activating your new phone. Keep it powered off while you're not using it.
- Don't use the burner's phone number for anything at all that isn't related to this specific project. This is called compartmentalization; if someone discovers the entire history of that phone number, they shouldn't be able to learn anything new.

- Each cellphone handset has a unique identifier. So if you need a second phone number at some point in the future and you don't want it to be connected to your first phone number, you'll have to buy a second handset.

After buying phone service, you'll need to activate the phone. This process will be different with different phone companies. TracFone requires you to activate your handset either by calling their phone number from a different phone — obviously not a good option for someone trying to remain anonymous — or by activating online at their website. I activated my burner phone online using Tor Browser.



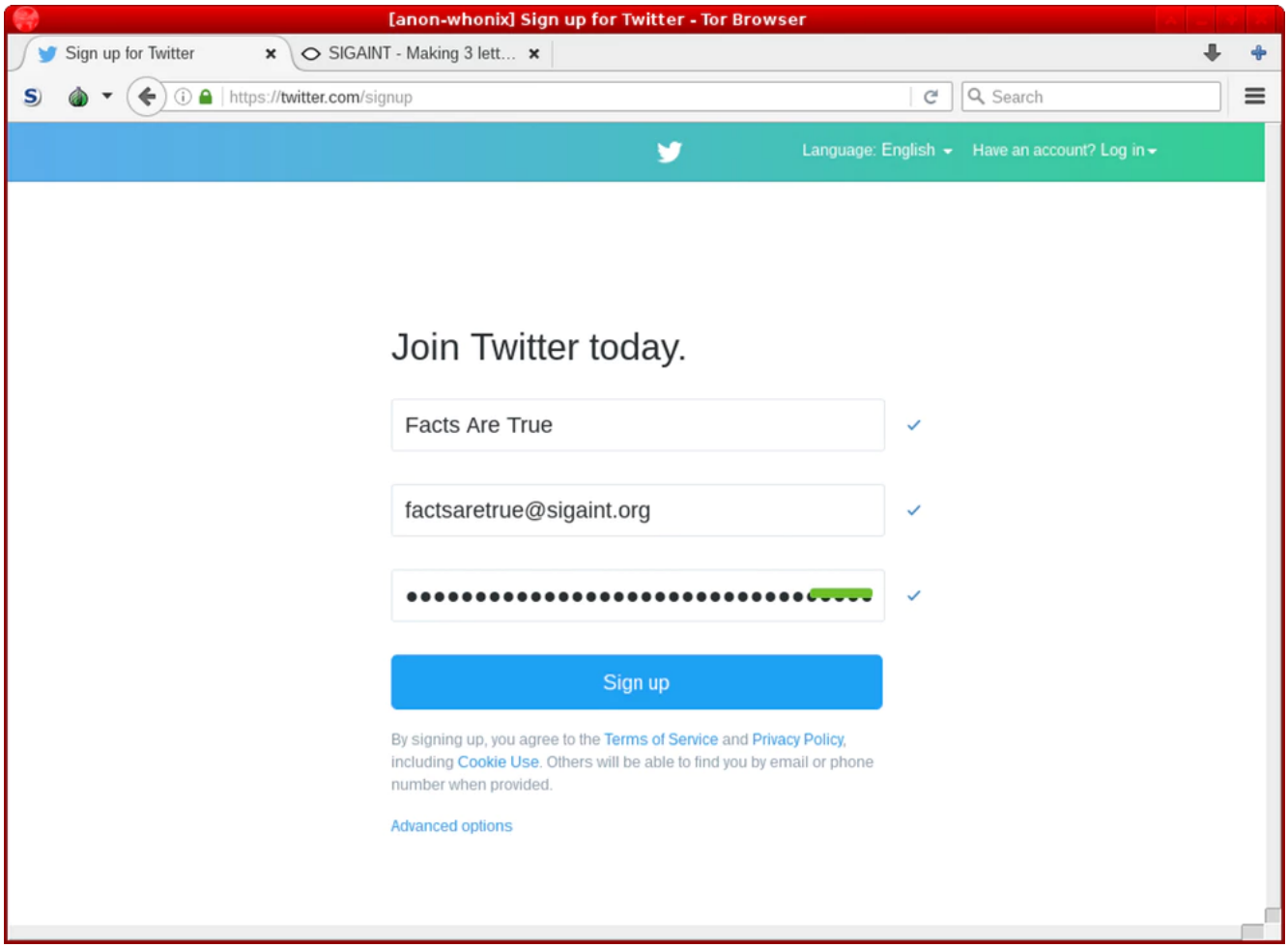
Once you've activated your phone, you can use the phone's menu system to learn what your new phone number is. On my LG 328BG, I pressed Menu, selected Settings, and finally Phone Information to find it.

Creating a Twitter account anonymously

Finally, armed with an email address and phone number that aren't in any way connected to my real identity, I could create a Twitter account.

Before making an account, grab your laptop and burner phone and go to a public location that isn't your home or office, such as a coffee shop. When you get there, power on your burner phone. Keep in mind that this location is now tied to your burner phone, so you might wish to do this step when you're traveling in another city.

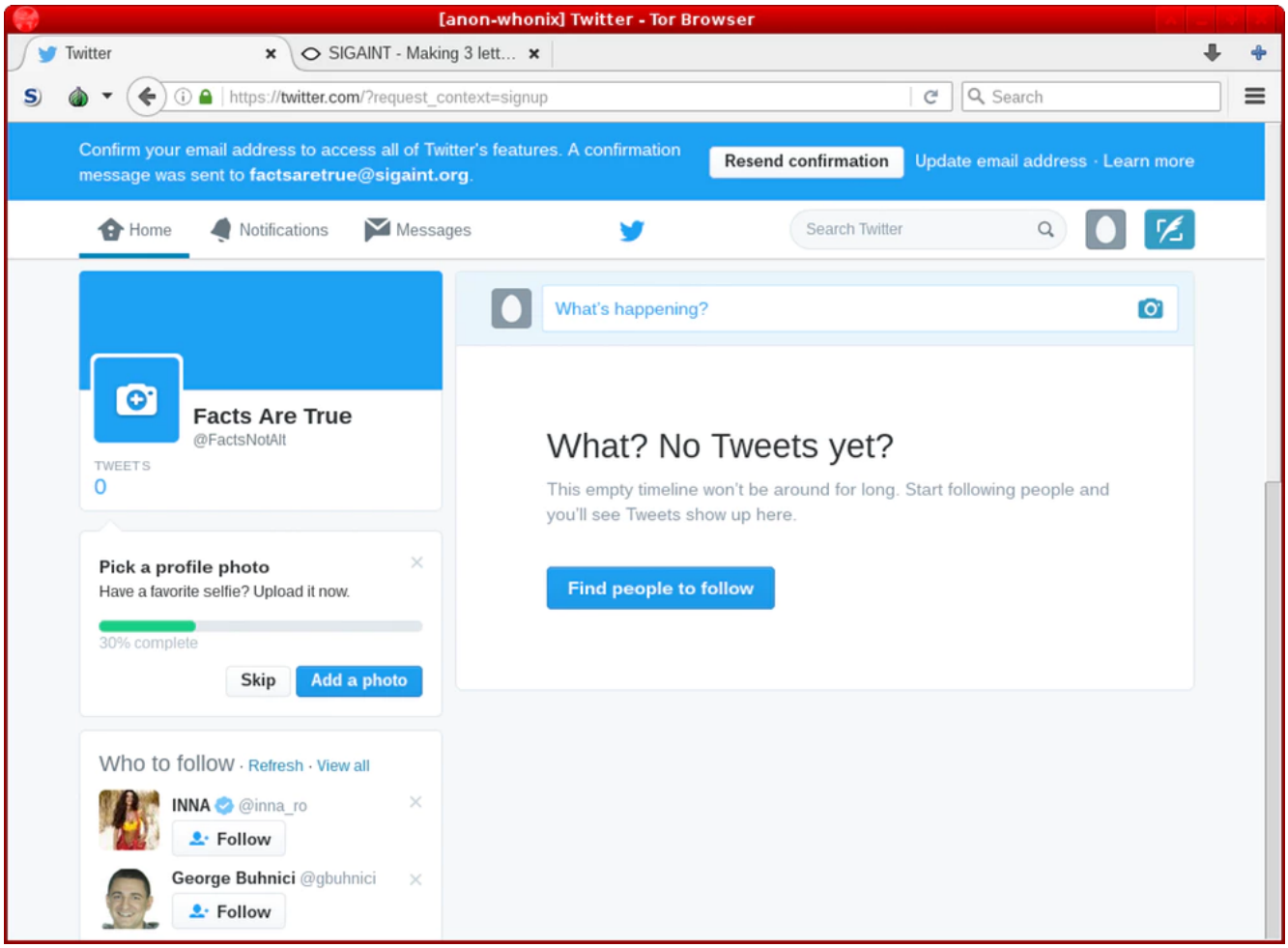
Using Tor Browser, I navigated to https://twitter.com/signup and signed up for a new account. The new account form asked for my full name ("Facts Are True"), my email address (factsaretrue@sigaint.org), and a password.



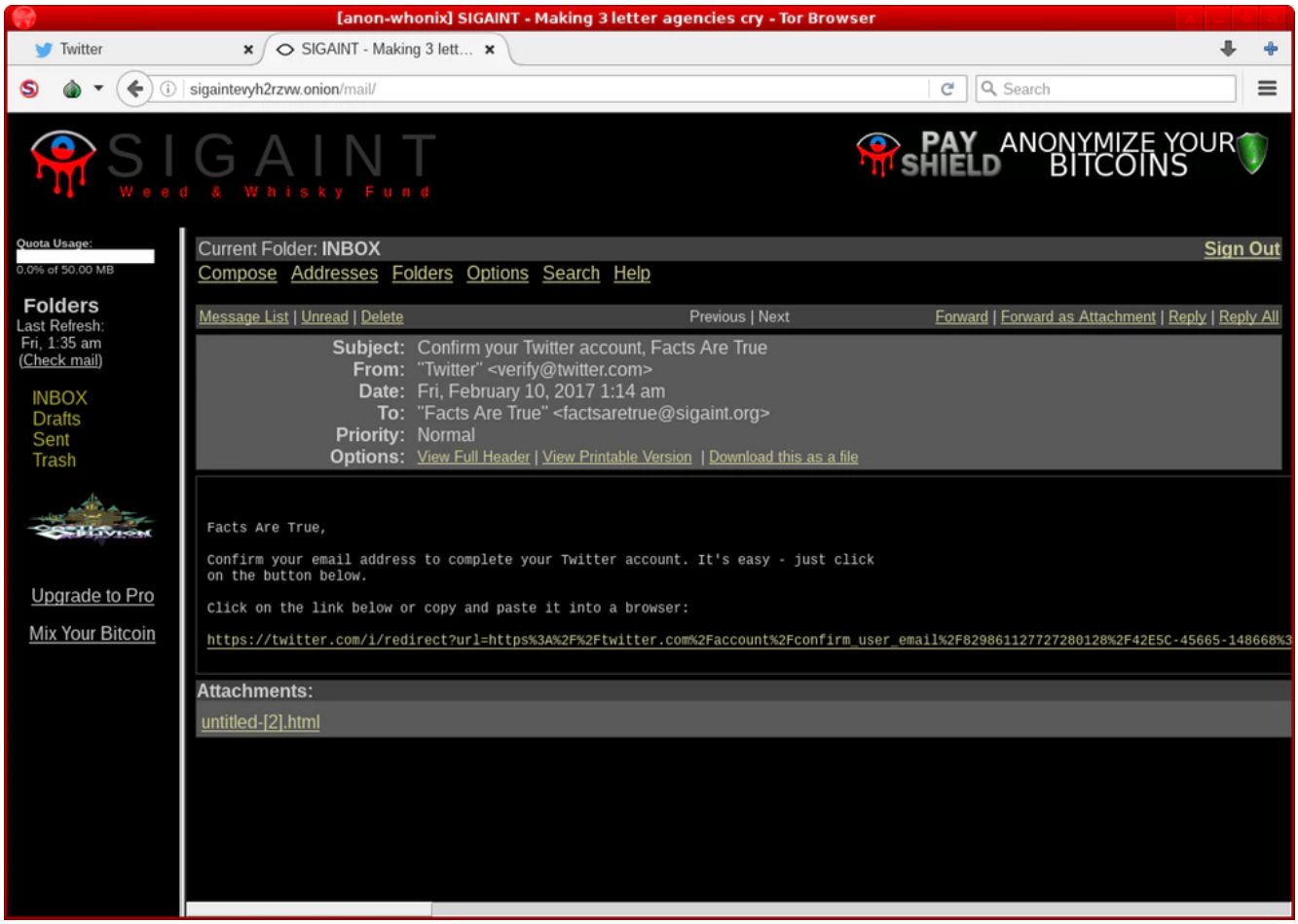
After clicking “Sign up,” I was immediately prompted to enter my phone number. I typed my anonymous phone number and clicked “Call me.” A Twitter robot called my burner and read out a six-digit number, which I typed into the next page on Tor Browser. It worked great.

With the phone number verification step complete, I powered off my burner phone. Once you’re sure you don’t need your burner phone anymore, it’s a good idea to get rid of it.

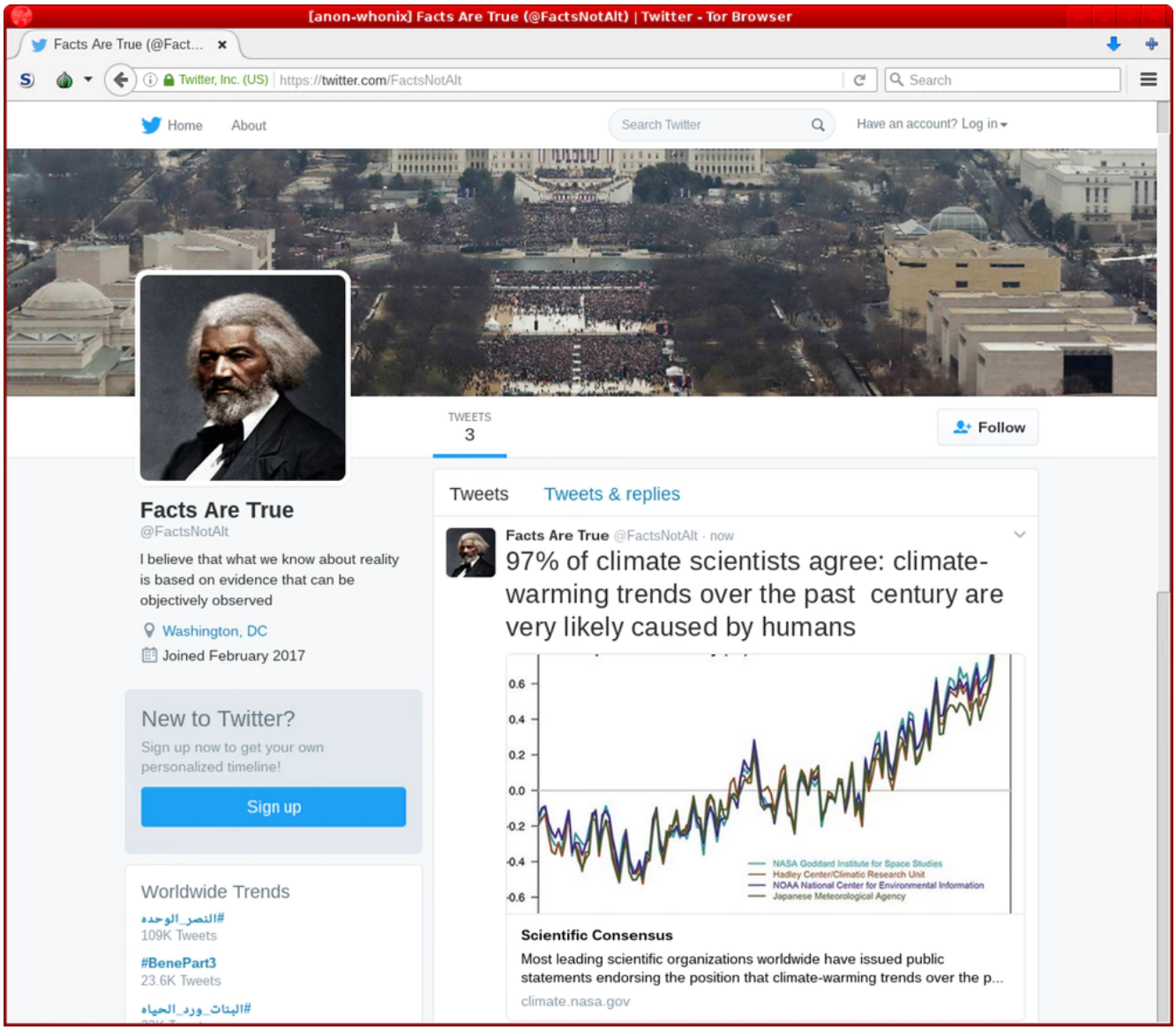
Toward the end of the signup process, Twitter prompted me to come up with a username. After many tries, I found one I liked: @FactsNotAlt. After clicking through the welcome screen, I was finally logged into my new anonymous account.



I went ahead and confirmed that I control my factsaretrue@sigaint.org email address.



And there you have it. I set up my new account and began tweeting about things that are true.



Maintaining the Twitter account over time

If you're following along, you've now created a completely anonymous Twitter account as well. Congratulations! But your work has only just started. Now comes the hard part: maintaining this account for months, or years, without making *any mistakes* that compromise your identity. I won't be following these tips myself with the @FactsNotAlt account – I've already outed myself as the owner. But for anyone who is trying to

anonymously maintain a popular Twitter account, here are some things to keep in mind.

Be careful about how you interact with people:

- You should operate on a strict need-to-know basis. Don't tell *anyone* who doesn't need to know that you're involved with running this account. Don't brag. This is, by far, the easiest way to mess up and for your real identity to come out: gossip.
- Be careful about what privileged information you tweet. If you're part of a small group of people who have access to some information and you tweet about it, you might become a suspect when before you weren't.
- If your account becomes popular, you might begin having conversations with lots of strangers on the internet. Be very careful what you say, even if you're saying it in a private message. Some of these strangers might be gaining your trust in hopes that you'll slip and tell them scraps of information about your identity.
- Be very careful about clicking links that people send you — they could be trying to learn your IP address, or even trying to hack Tor Browser. Avoid clicking them at all, but if you really want to click one, first make sure you're running the very latest version of Tor Browser and set your security slider to High.
- Be conscious of your word choice. People might analyze your writing style to de-anonymize you, so you should try to write in a voice that's distinct from your own, if you can. For example, it wouldn't be wise for Donald Trump to tweet, "The failing @theintercept keeps writing FAKE NEWS. Sad!" from his anonymous account, because people might suspect that he's the person behind that account.

Compartmentalize:

- Never log in from your work computer — many companies spy on their employees' computers. Use a personal computer instead. Also,

avoid your work network — many companies log exactly which computers connect to their network and what they do online. Tor hides what you're doing, but the company can still tell that you're using Tor on their network.

- *Always* use Tor Browser when using your account. Don't log in on your phone. Don't log in with any other browser. Don't even look at your anonymous Twitter account while logged in to your personal account.
- When you are logged in to your anonymous account, don't follow your personal account, or the accounts of any of your friends. Don't retweet or like any of those tweets either. Basically, don't make it obvious who your social group is.
- Be careful about uploading photos for tweets or your profile. Photos often contain metadata that could be used to lead back to you. Screenshots don't though, so one easy way to remove metadata from a photo is to take a screenshot of it.

Many successful Twitter accounts have a team of people who run them instead of a single individual. If you're part of such a team, or thinking of sharing access to your existing account with someone new:

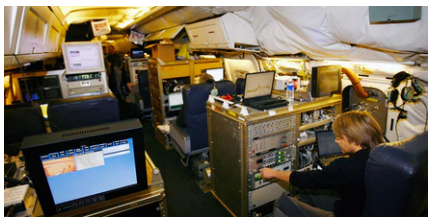
- Only invite people who you know and trust.
- Come up with a set of operational security rules — like the rules listed above — and make sure that everyone involved understands them and is on the same page.
- Come up with a secure communication channel as a team, and only discuss the Twitter account using this channel, or in person. There are many different technologies you could use, all with different trade-offs, but one option is to use the encrypted messaging app Signal: Create a Signal group (with an innocuous name) and set your messages to automatically disappear after a short time, like five minutes.

- Instead of just tweeting when you come up with ideas, edit each other's tweets. This will both improve the quality of the tweets and could help defeat style analysis, since you'll end up with a shared voice.

And finally, keep in mind that after all this, Twitter can always kick you off for their own reasons. And if your account gets hacked and the email address associated with it is changed, you'll have no way to recover it.

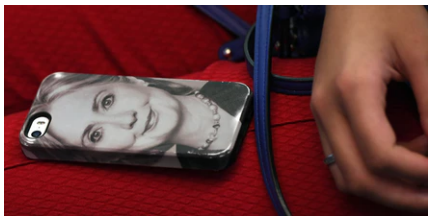
Good luck!

RELATED

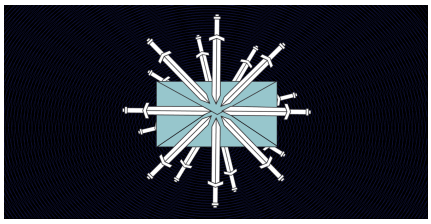


How Scientists Can Protect Their Data From the Trump Administration

Surveillance Self-Defense Against the Trump Administration



Dear Clinton Team: We Noticed You Might Need Some Email Security Tips



Security Tips Every Signal User Should Know