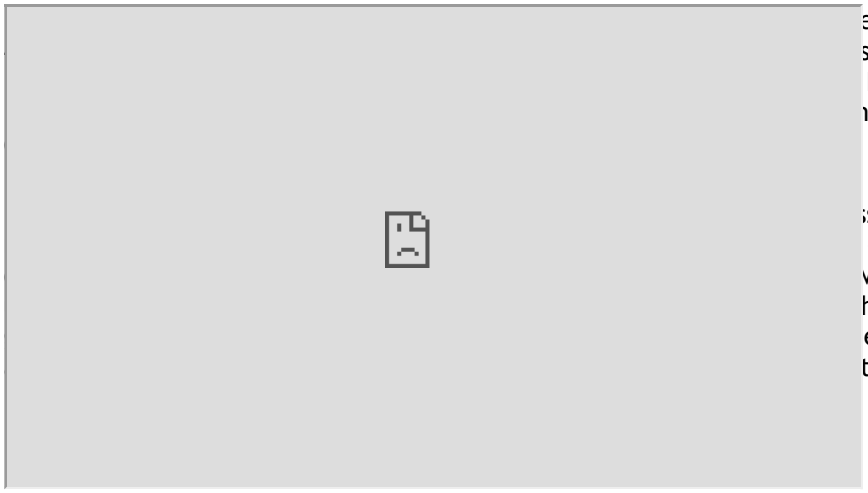
Ignored By Big Telecom, Detroit's Marginalized Communities Are Building Their Own Internet

40 percent of Detroit residents don't have any access to internet at all.

Kaleigh Rogers
Nov 16 2017, 7:50am

Being stuck without access to the internet is often thought of as a problem only for rural America. But even in some of America's biggest cities, a significant portion of the population can't get online.

Take Detroit, where 40 percent of the population has no access to the internet—of any kind, not only high speed—at home, [according to the Federal Communications Commission](). Seventy percent of school-aged children in the city are among those who have no internet access at home. Detroit has one of the most severe digital divides in the country, the FCC says.



e and how
see how
Diana
ne at her

sroots
coalition of
vith three
hared
e street,
the

Image: Lara Heintz

The issue isn't only cost, though it is prohibitive for many Detroiters, but also infrastructure. Because of Detroit's economic woes, many Big Telecom companies haven't thought it worthwhile to invest in expanding their network to these communities, Nucera told me. The city is filled with dark fiber optic cable that's not connected to any homes or businesses—relics from more optimistic days.

Residents who can't afford internet, are on some kind of federal or city subsidy like food stamps, and students are prioritized for the Initiative, Nucera told me. The whole effort started last summer with enlisting digital stewards, locals from each neighborhood who were interested in working for the nonprofit coalition, doing everything from spreading the word, to teaching digital literacy, to installing routers and pulling fiber.

Image: Lara Heintz

Many of these stewards started out with little or no tech expertise, but after a 20-week-long training period, they've become experts able to install, troubleshoot, and maintain a network from end to end. They're also aiming to spread digital literacy, so people can truly own the network themselves.

"We want to make sure that we're not just installing all the equipment, but also educating the community," said Rita Ramirez, one of the stewards working on the project in Detroit's Southwest neighborhood.

One component the groups are most eager to build out is the intranet that will result from connecting so many homes (about 50 in each neighborhood) to a shared wireless connection. They are encouraging local residents to take advantage of that intranet and build shared tools like a forum and emergency communication network that is completely localized and secure.

In a city that is rebuilding after a decade of economic turmoil, the internet can no longer be a luxury for the wealthy. Detroit's renaissance won't happen without each of the city's diverse communities having access to the basic tools of modern work, education, healthcare, and communication. All of Detroit (or, certainly, more than 60 percent) needs access to the internet and the current structure established by Big Telecom hasn't made this an easy goal.

"Communication is a fundamental human right," Nucera said. "This is digital justice."

Dear Future is a partnership with CNET that will explore the people, companies, and communities that are ushering in the future we were all promised. Follow along here.

Email Address

SUBSCRIBE

SIGN UP FOR MOTHERBOARD PREMIUM.

Find us in the future.

LIKE MOTHERBOARD

HOW HACKING WORKS

The Motherboard Guide to Avoiding State Sur

A straightforward guide to privacy, messaging, and keeping yourself safe from passive and active surveillance.

Sarah Jeong
Nov 27 2017, 8:30am

Image: Koji Yamamoto

This is excerpted from the Motherboard Guide to Not Getting Hacked, our comprehensive guide to digital security. We recommend you read that entire guide if you are generally looking to improve your privacy and security—if you do not take basic steps such as using unique passwords for every account and enabling two-factor authentication on your accounts, this guide will do little to help you. This guide, and that one, will be regularly updated. This post was last updated November 14. -Jason Koebler

In the wake of September 11th, the United States built out a massive surveillance apparatus, undermined constitutional protections, and limited possible recourse to the legal system.

Given the extraordinary capabilities of state surveillance in the US—as well as the capabilities of governments around the world—you might be feeling a little paranoid! It's not just the NSA—the FBI and even local cops have more tools at their disposal to snoop on people than ever before. And there is a terrifying breadth of passive and unexpected surveillance to worry about: Your social media accounts can be subpoenaed, your emails or calls can be scooped up in bulk collection efforts, and your cell phone metadata can be captured by Stingrays and IMSI catchers meant to target someone else.

Remember, anti-surveillance is not the cure, it's just one thing you can do to protect yourself and others. You probably aren't the most at-risk person, but that doesn't mean you shouldn't practice better security. Surveillance is a complicated thing: You can practice the best security in the world, but if you're sending messages to someone who doesn't, you can still be spied on through their device or through their communications with other people (if they discuss the information you told them, for instance).

That's why it's important that we normalize good security practices: If you don't have that much to be afraid of, it's all the more important for you to pick up some of these tools, because doing that will normalize the actions of your friends who are, say, undocumented immigrants, or engaged in activism. Trump's CIA Director thinks that using encryption "may itself be a red flag," If you have "nothing to hide," your use of encryption can actually help people at risk by obfuscating that

red flag. By following this guide, you are making someone else safer. Think of it as herd immunity. The more people practice good security, the safer everyone else is.

The security tips provided earlier in this guide still apply: If you can protect yourself from getting hacked, you will have a better shot at preventing yourself from being surveilled (when it comes to surveilling iPhones, for instance governments often have few options *besides* hacking the devices). But tech tools don't solve all problems. Governments have a weapon in their hands that criminal hackers do not: the power of the law. Many of the tips in this section of the guide will help you not only against legal requests and government hacking, but also against anyone else who may be trying to spy on you.

You don't have to turn yourself into a security expert. Just start thinking about your risks, and don't be intimidated by the technology. Security is an ongoing process of learning. Both the threats and the tools developed to address them are constantly changing, which is one of the reasons why privacy and security advice can often seem fickle and contradictory. But the tips below are a good starting point.

Threat Modeling (privacy and surveillance edition)

Keep in mind that different tools address different problems. Without threat modelling, it's easy to feel overwhelmed by how many tools are out there. Threat modeling for surveillance is similar to threat modelling for hacking, but there are of course some nuances that vary in every situation.

It's easy for some people to say "use Signal, use Tor," and be done with it, but that doesn't work for everyone. For example, a friend used to message people about her abusive ex-partner using the built-in *Words With Friends* messenger, because she knew that he read her text messages and Gchats. *Words With Friends* does not have a particularly secure messaging system, but in this case it was a better option than Signal or Hangouts because he didn't think to read her messages on the game.

When it comes to state actors, it might be helpful to think of surveillance in two different forms: surveillance of metadata (who you are, who you're talking to, when you're talking) and surveillance of content (what you are saying). As with all things, when you dig a little deeper, it's not as simple as that. But if you're thinking about this for the first time, it's a good start.

Surveillance law is complicated, but long story short, both the law and current technological infrastructure make it easier to grab metadata than content. Metadata isn't necessarily **less important or revealing** than content. Say Planned Parenthood called you. Then you call your partner. Then you call your insurance. Then you call the abortion clinic. That information is going to be on your phone bill, and your telephone provider can easily give it up to the government. Your cell provider might not be recording those calls—the content is still private. But at that point, the content doesn't matter—it would be easy for someone with the metadata alone to have a reasonable idea of what your calls were about.

Start thinking about what is open and exposed, and what you can protect. Sometimes, you have to accept that there's very little you can do about a particular channel of communication. If circumstances are dire, you're going to just have to work around it.

Signal

Signal is an encrypted messaging service for smartphones and desktop computers. It is, for many—but not all—people, a good option for avoiding surveillance. Because the government has the capability to intercept electronic messages while they're being transmitted, you want to use end-to-end encryption for as many of your communications as possible.

Using Signal is easy. You can find it and install it from your phone's app store. (In the iOS App Store and the Google Play Store, it's called "Signal Private Messenger," and it's made by Open Whisper Systems.)

If you have the other person's phone number in your contacts list, you can see them in Signal, and message them or call them. As long as the other person also has Signal, the messages automatically encrypt—all the work is invisible.

It even has a desktop app, so you can use it the way that iOS/Mac OS people use iMessage on both their phones and computers. Go to the Signal.org website and download the app for your preferred operating system. Just follow the instructions —trust us, they're easy.

Signal also lets you set a timer for messages to automatically expire, thus deleting them from all devices. You can set the timer for all kinds of lengths, including very short ones. This is a great feature for journalists who are concerned about protecting their sources or their conversations with editors.

These are great features, and they're part of the reason why we recommend Signal over many other end-to-end messaging apps. iMessage and WhatsApp also use end-to-end encryption, but they both have drawbacks.

We do not recommend WhatsApp, because WhatsApp is owned by Facebook, and has been sharing user information with its parent company. While this is only metadata, it is ultimately a rollback of a privacy promise made when WhatsApp was acquired by Facebook. We think this says something negative about the overall trustworthiness of the company in coming days.

It is a very good thing that Apple encrypts iMessages end-to-end. But iMessage also backs up messages to iCloud by default, which is why you can message from all your Apple devices. This is a great and fun feature, but if you're concerned about government surveillance, remember that Apple complies with lawful government demands for data in your iCloud: "iMessage and SMS messages are backed up on iCloud for your convenience," Apple's privacy page states. You can turn this feature off, but in theory Apple could be forced to access the iMessages you've sent people who still have the feature enabled.

Signal keeps very little information. We know this, because Open Whisper Systems was subpoenaed by the government last year, and was forced to hand over information. But the information it had—by design—was pretty minimal. Signal retains phone number, account creation date, and the time of the user's last

connection to Signal servers. Yes, that's still something, but as you can see, it's not very much.

There are worse products to use than iMessage and WhatsApp. For example, you absolutely should avoid using Telegram for sensitive communications. And Google can read your GChats unless you take additional steps to encrypt them end-to-end. There are several other products on the market that are decent alternatives (for example, Wire), but like WhatsApp and iMessage, they're created and maintained by for-profit companies, and we don't know how they're planning to monetize in the future. Signal is an open source, nonprofit project. That has its own drawbacks (for example, Signal is not as slick as iMessage, nor does it have the luxury of having a large security team behind it), so maybe donate money when you download it?

One thing that's worth mentioning about Signal is that it requires you to associate the device with a phone number. This means that you need to trust the people you're messaging to have your phone number (or need to jump through hoops to use Signal with a dummy phone number); there are many reasons why you might want to message people without giving them your phone number, which is one of the potential drawbacks of Signal. If this is a concern for you, consider another option.

Another thing to remember is that just because a communication is end-to-end encrypted doesn't mean it's invisible to the government. It just means the contents are encrypted *between* endpoints. You can see the message, your recipient can see the message. If it's intercepted in transit, it's completely garbled, and the content of your message is protected from spying eyes.

But if an "endpoint" is compromised—in other words, if your own phone is hacked or physically seized by the government, or your texting partner is screencapping your conversation—it's game over.

Encryption doesn't make it impossible for the government to snoop, it just makes it way more challenging. The point is that introducing friction into the equation does provide privacy.

Be conscious of what you post on social media

If you post publicly on social media, know that local police (and likely federal agencies as well) keep tabs on activists online. For example, Facebook, Instagram, and Twitter have all fed data to social media monitoring products that police departments used to track Black Lives Matter activists.

Even if you keep your privacy settings on lockdown, social media companies are subject to subpoenas, court orders, and data requests for your information. And often times, they'll fork over the information without ever notifying the user that it's happening. For the purposes of social media, assume that everything you post is public. This doesn't mean you should stop using social media, it just means you have to be mindful of how you use it.

If you're an activist, consider using a pseudonym for your activism. If you post online at all, take others' safety and privacy into consideration as well.

Who are you tagging into your posts? Are you adding location information? Who are you taking a picture of, and why? Be particularly careful with photos or posts about protests, rallies, or meetings. Facial recognition technology is fairly sophisticated now, so even if you leave people untagged, theoretically an algorithm could scan for and identify activists in a photograph of a rally. You can already see this at work in Facebook's tag suggestions.

When you take a picture of someone at a protest, make sure that they consent, and that they know the implications of having a photo of themselves out there.

Beware of device cameras and microphones

Do you live around any cameras? If you use internet-connected security cameras inside your home, or have a webcam running, don't leave these things unsecured. Make sure that you've changed any passwords from the default that they shipped with, and cover them when you're not using them.

If you have a laptop or a smartphone, use a sticker to cover the front-facing camera. You don't have to stop Facetiming and taking selfies, you just want to cover things up so no one's looking at you when you don't want them to. The Electronic Frontier Foundation sells removable laptop cover stickers (five for $5) that won't leave a residue on your camera, so you can take it on and off whenever you need it. Consider buying several and giving them to friends who might be shorter on cash.

Finally, there is absolutely no way to make sure your microphone is not recording. If you're concerned about being wiretapped, consider turning off your phone and putting it in the microwave (**temporarily, with the microwave off**), or leaving your phone in the other room. Turning your phone off alone does not necessarily protect you! And consider leaving all your devices outside of the bedroom when you have sex with your partner.

In 2012, Khadija Ismayilova, an Azeri journalist, was blackmailed with a surreptitiously filmed sex tape. The blackmailer told Ismayilova to stop publishing articles critical of the government, or else have her tape released. (Ismayilova went public, and the tape was posted on the internet.) In 2015, the Azerbaijan government sentenced her to seven and a half years in prison on tax evasion charges. She is currently out on probation.

Governments at home and abroad have used sex to blackmail dissenters. Be aware of that, and protect your privacy.

Protect your devices with a lock screen

Put a password/passcode on your phone and your computer. Don't rely on your thumbprint alone. The police are more likely to be able to legally compel you to use your fingerprint to open up your phone. You may have a stronger constitutional right not to speak your password.

Use OTR for chatting (if you have to)

It's best to use Signal for desktop when chatting with people. But here's another option that's particularly useful for journalists.

Close your Gmail window and use OTR (Off The Record) instead to chat. Keep in mind that you can only use OTR if the other person is also using OTR. Mac users can **install Adium**, PC (and Linux) users will have to **install Pidgin and the OTR plugin**.

You can use your Gmail account as your chat ID. So what's going on is that you're engaging in Gchat, but with a layer of encryption on top. Open up a chat window and click the lock icon to begin encryption. And make sure you tweak your settings so that you're not retaining chat logs during encrypted conversations.

Again, end-to-end only goes so far. **If the other person is logging your conversations**, it might not matter that you went this far. If you're concerned, ask your friend to stop logging.

Install the Tor Browser

Tor—which takes its name from an acronym for "The Onion Router"—scrambles your internet traffic by routing it through several layers of computers. This way, when you access a website, it can't tell where you're connecting from. The easiest way to use Tor is just to install the Tor Browser. It's just like Firefox or Chrome or Internet Explorer, just a lot slower because of the privacy it provides.

Using Tor for everything will give you a big privacy boost, but it's a bit unwieldy. Don't, for instance, try to stream Netflix over Tor.

Evaluate your needs and figure out how much Tor you need in your life. Always remember that your IP address (which can give away where you are, and therefore, who you might be) is laid bare if you aren't using it.

There are four reasons why you might want to use Tor.

- You're trying to keep your identity hidden.
- You use a lot of public WiFi.
- You're trying to get around government censorship.
- You are protecting the other people who use Tor.

If you're an activist who is trying to hide their identity, you need Tor to mask your IP address. This is a limited use case scenario. For example, it's self-defeating for me to open up Tor, log into my public Twitter account, and tweet, "What up, everyone, I'm tweeting from the Vice Media offices in New York City." I am giving away all the information that Tor is masking for me—because when it comes down to it, in that use case scenario, I was never planning on keeping it private.

If you connect to a lot of public Wi-Fi (think Starbucks, a hotel, or the airport), though, you should use Tor. It provides similar benefits as VPNs , but without many of the drawbacks of a VPN (see the next section for a discussion of that).

If the United States begins to censor parts of the web, as many other governments do, Tor might be able to help you get around that. Tor certainly helps people connecting to the internet from other countries that practice internet censorship.

Finally, the thing about Tor is that the more people use it, the less trackable everyone else is. When a lot of random, unaffiliated people from all over the world use it, it becomes stronger and stronger. If you take the time to use Tor every day, you are helping people who really do need it.

A couple caveats, here: Tor is not bulletproof. The government has been known to hack groups of users on Tor, just like it's been known to hack VPN users en masse. Tor, by itself, does not make it more unlikely for you to get hacked. Tor is for privacy, not security. And Tor is designed to make it *hard* to log your traffic, not*impossible*, so there's always a risk that you aren't being hidden.

The computers that make up the Tor network—the ones that your traffic bounces through—are run by volunteers, institutions, and organizations all over the world, some of whom face legal risks for doing so. They are not supposed to log the traffic that goes through them, but because it's a volunteer network, some might. The risk is mitigated by the fact that each node only sees a snapshot of the traffic running through it, and nobody has access to both the user's IP and their unencrypted traffic. A bad actor would have to run a very large number of Tor nodes to start logging meaningful traffic—which would be difficult—and the Tor project monitors for behavior that suggests anybody might be doing that.

Ultimately, for the purposes of state surveillance, Tor is better than a VPN, and a VPN is better than nothing.

It's not clear whether Tor will continue to exist into the future. Tor is run partly through grants from the government. (Like many cutting edge technologies, Tor was originally developed by the US military.) It's possible Tor will lose most of its funding in the very near-term. Consider donating to the Tor Project.

Virtual Private Networks

When it comes to state surveillance, VPNs won't help much. A VPN will obscure your IP address, but when it comes to state surveillance, VPNs can be subpoenaed for user information that may ultimately identify you. For example, many VPN companies keep logs on what IP addresses log on when and what sites are accessed—which can end up pinpointing you, especially if you used your credit card to pay for a VPN subscription.

Some VPN companies claim not to log user information. You need to evaluate how much you trust these companies, and make that decision for yourself. If what you're concerned about is government surveillance, our recommendation is that you stick with Tor.

PGP (probably isn't worth the trouble)

The only reliable way to encrypt your email is PGP—also known as Pretty Good Privacy. However, PGP is incredibly obnoxious to use. Even PGP's creator Phil Zimmermann has stopped using it, since he can't use it on his phone. The problem isn't just that *you* have to figure out PGP, everyone you talk to also has to figure it out. Telling someone to download Signal is a lot easier than walking them through public/private key encryption. This is where your threat model comes in handy, to help figure out if PGP is actually worth it to you.

If you absolutely must use encrypted email, this guide to PGP might be helpful. It's tricky, so you might want to go to a crypto party and have an activist or technologist help you set it up.

Don’t run your own email server

If 2016 did anything, it convinced everyone not to run their own private email server.

It’s true that Google and other companies have to comply with court orders for your information, including your emails. But on the other hand, Google knows how to run email servers way better than you do. Email servers are hard! Just ask Hillary Clinton.

If you are encrypting email, Google can only hand over the metadata (who’s sending to whom and subject headers). Since encrypting email is a huge pain, try to keep all your sensitive stuff away from email, and in end-to-end encrypted channels instead. Don’t abandon your third-party email account, just be aware that the government can get at what’s inside.

Encrypt your hard drive

Good news: this isn't as hard as it used to be!

Full-disk encryption means that once your device is locked (when it's off, or when it's on but showing a lock screen), the contents of your hard drive can't be accessed without your password/key.

A lot of smartphones come with full disk encryption built in. If you own an iPhone with a recently updated operating system (like, in the last three years, really), just slap a passcode on that sucker and you're golden.

If you own an Android phone, it might already be encrypted by default (Google Pixel is). But chances are, it's not. There isn't an up-to-date guide on turning on encryption on all Android devices, so you're going to have to poke around yourself, or ask a friend. And if you own a Windows phone, god help you, because I can't.

As for computers, things are again, much easier than they used to be. Use your operating system's full disk encryption option instead. For MacBooks running Lion or newer, just turn on FileVault.

Windows, on the other hand, is a lot more complicated. First off, *some* users have encryption by default. Some more users can turn it on, but it's kind of a pain. And if you're using Microsoft's Bitlocker, you're going to have to fiddle with some additional settings to make it more secure. Apple doesn't retain the capability of unlocking your devices. Famously, if the government goes to Apple, Apple can't just decrypt your phone for the feds, not without coming up with a hack that will affect every iPhone in the world. But Microsoft isn't doing quite the same thing—in some cases they use what's known as "key escrow," meaning they can decrypt your machine—so you have to take additional steps (outlined in this article) to get that same level of protection.

You may need to resort to using VeraCrypt. A lot of older guides will say to use TrueCrypt, regardless of operating system. This is now outdated advice. VeraCrypt used to be TrueCrypt, and the story of why it's not any more is a convoluted crypto soap opera with plot holes the size of Mars, and it is frankly outside the scope of this guide. Long story short, there's nothing wrong with VeraCrypt as far as the experts can tell, but if you have the option, use the full disk encryption that your operating system already provided.

If you use Linux, your distro probably supports encryption out of the box. Follow the instructions while installing.

If you're a journalist, know the risk of hanging onto your notes

Want to protect your sources? Your notes, your Slack chats, your Gchats, your Google Drive, your Dropbox, your recorded interviews, your transcripts, and your texts can all end up in court. Depending on what kind of court case it is, it might not matter that it's encrypted.

Don't wait until a lawsuit is imminent to delete all your stuff. That might be illegal, and you might be risking going to jail. Every situation is different: your notes might be necessary to get you *out* of trouble. So if you're the type to hoard notes, know the risk, talk to a lawyer, and act responsibly.

Credit Cards

Know that credit card companies never stand up to the government. If you pay for anything using your credit card, know that the government can get that information pretty easily. And remember that once your identity touches something, there's a chain that the government can follow all the way back.

For example, if you get a prepaid Visa gift card using your personal credit card, and pay a VPN company with that, the government can just go backwards through the chain and find your personal credit card, and then you. If you pay a VPN company with Bitcoin, but you bought the Bitcoin through a Bitcoin exchange using your personal credit card, that's traceable as well.

This applies to anything else you use money for, like buying domains or cheap, pay-as-you-go phones, known as burners. Practically speaking, there's not a lot you can do about this. It's one of the reasons why we recommend Tor instead of a VPN service.

It's also one of the reasons why it's so hard to get a burner phone that's *really* a burner. (How are you going to pay for continuing phone service without linking your name to it?) There is no easy answer here. We're not going to pretend to be able to give good advice in this instance. If you find yourself in a situation where your life depends on staying anonymous, you're going to need a lot more help than any internet guide.

One more thing: For now, organizations like the ACLU and NAACP have a constitutional right to resist giving up the names of donors. But your credit card or PayPal might betray you anyways. This doesn't mean you *shouldn't* donate to organizations that resist oppression and fight for civil rights and civil liberties. Rather, it makes it all the more important that you do. The more ordinary people do so, the more that individual donors are protected from scrutiny and suspicion.

We don’t know what the future holds

Which brings us to our next point: we don’t know what the future holds. This guide was written with the current technical and legal capabilities of the United States government in mind. But that might all change in the future. Strong encryption might become illegal. The United States might begin to practice internet censorship the way that China and other countries do. The government might institute a National ID policy for getting online, making it near-impossible to post anonymously.

These things are harder to enforce and implement, so they’re not likely to happen quickly.

It’s also not infeasible that the government pressures app stores to take down Signal and other end-to-end encryption applications. This guide might be only be so good for so long. That’s all the more reason to become proactive against surveillance now, and to keep adapting to changing circumstances.

Meet in person

Many public places have cameras, some spots are wired with microphones. And there's always the possibility that you are being individually targeted for surveillance. But ultimately, it's a lot harder to surveil someone in person than to collect the electronic communications of many people at the same time.

Take a break from the wired world and meet people in person. If you stay out of earshot, you won't be overheard, and your words will melt into the air, unsurveilled and unrecorded.

And besides, if you're reading this guide, chances are that you really need a hug right now.

So meet up with your friends, verify your Signal keys, and give each other a big hug. Because you're probably both scared, and you need each other more than you need any of this technology.

GO OUT THERE AND BE SAFE

That is all for now. Again, this is just meant to be a basic guide for average computer users. So if you're a human rights activist working in a dangerous country or a war zone, or an organization building IT infrastructure on the fly, this is certainly not enough, and you'll need more precautions.