# Anonymous and Encrypted Phones: Is it Possible?

By: Shane Radliff

April 3rd, 2016

Liberty Under Attack

Mass surveillance is an epidemic that has been plaguing privacy advocates for decades. One of the most pervasive forms is the dragnet wiretapping of telephones. According to the Pew Research Center, over 90% of American adults own a cell phone, and amongst those owners, 64% own a smartphone. Not only do government snoops have access to all of your calls, but due to the advent of the smartphone, datamining and intelligence gathering has never been easier—it's a one-stop shop for Leviathan.

That said, one of the categories on The Freedom Umbrella of Direct Action is security culture, which can be defined thusly:

> ***"Security culture is the direct application of the right to privacy."***

One of the items in that category, is anonymous cell phones. This includes the use of payphones, "burner" phones, and encryption applications on smartphones. The goal of this article is to analyze each of those items, in regards to the cost, the efficacy, and the user-friendliness of the various methods. The ultimate question to be answered is this: **Is it possible to browse the Internet and talk anonymously using telephones?**

## Payphones

It feels strange even mentioning this concept, as they largely died out during my lifetime. The most recent statistics show that there are about 250,000 payphones left in the United States. As seen in *Better Call Saul*, there is still the possibility of anonymity using payphones; that is, if you can find one. For me personally, I have not seen a payphone in Bloomington/Normal in the almost ten years that I've lived here.

That said, if there is a payphone near where you live, it can certainly be used for coordinating mail drops or discussing any other matter that you wouldn't want government snoops to hear about. The only real privacy an individual can expect from a payphone, besides the fact that it is not tied at the hip to your legal identity, is combining the use of one with pre-paid phone cards that were bought with cash.

Granted, a record of any calls made using such phone cards is maintained with the card vendor, however, mixing and matching a variety of phone cards could make it quite difficult for a skip tracer to track down your movements; at most, he would be chasing an elusive smell, if you did it right. Unfortunately, the ability to place a "collect call" when considered as a parallel to the diminishing availability of payphones, renders this once useful method as simply being outdated for maintaining any sense of privacy, except in the most rare of circumstances.

In summation, the prevalence of payphones in today's digital world is not only slim, but renders their use value to almost nothing, simply due to the fact that their growing extinction, when considered alongside newer options, greatly diminishes their marginal utility.

**"Burner" Phones**

Is it possible to retain individual privacy while using a no-contract phone service? The answer is "yes."

If you want to purchase a prepaid ("burner") phone, you can do so using cash. Following that, you must activate the phone; however, what personal information is required, if any at all? Additionally, what are the costs of the various plans? This chart should answer these questions. *(Note: The company names will either have the transcript or the recording of the phone call linked for verification purposes. Unfortunately, I was unable to record the phone call for Verizon.)*

| Provider | Average Cost | Activation Information |
|---|---|---|
| **Straight Talk** | $30 | Zip Code Only |
| **Verizon** | $30 | Zip Code Only |
| **AT&T** | $30 | Zip Code/Lie About the Rest |
| **T-Mobile** | $40 | Date of Birth and Pin Number |

On a purely "consumer report" basis, I would rank the companies as such:

1. **Straight Talk**: Certainly not a major company like Verizon or AT&T, but they provide 24/7 customer service.
2. **T-Mobile**: Again, not a Verizon or AT&T, yet they also provide 24/7 customer service.
3. **Verizon**: Nothing special here, just a shorter wait time than AT&T.
4. **AT&T**: I was placed on hold for 20 minutes to ask one question.

With that said, it was interesting to hear the initial answers to my question of, "I am a privacy advocate, so I was wondering what personally identifiable information is necessary to activate the cell phone?" Ultimately, the first answer was mostly "name, address, zip code, and a pin number", although, when I pushed a little harder, I got similar answers from every company. Essentially, **no personally identifiable information is necessary to activate a prepaid phone**,

and the lady from AT&T even mentioned that I could lie when providing information, or just not provide it at all.

In summation, the costs are predominantly similar as well, which can be seen in the chart. T-Mobile is a bad deal, as you can get the same plans for less with the other companies.

But, what about the legality? As far as I know, there are no laws or regulations in place mandating anyone to present government identification to acquire a prepaid phone. In actuality, on March 23rd, Congresswoman Jackie Speier introduced a bill into the House of "Representatives" that would require government identification to purchase a prepaid phone. That said, government is slow and I wouldn't envision this bill passing, nor would I halt any plans of purchasing a prepaid phone due to the bill's introduction. If anything, on the off chance that her bill does survive the legislative process by becoming government law, all that would mean is that *now* is the time to invest in a "burner" phone (if not two or more).

There are a couple of points worthy of pointing out if you do decide to use a "burner" phone. Since you are more than likely doing it for privacy concerns, and would withhold personally identifiable information, you lose customer service if something goes wrong, unless you decide to provide personal information later on, but that would make the entire process a moot point, if your goal is privacy.

The final point here is with regards to using encryption applications on pre-paid smartphones. Now, obviously, it would not be wise to use your personally identifiable information on encryption applications to begin with, but it would be especially stupid to do so on a pre-paid phone, since that would be very counter-productive.

**Encrypted Messaging and Phone Calls**

There are a number of applications on the Apple Store that ensure privacy and anonymity when it comes to instant messaging, secure browsing, and encrypted telephone calls. Personally, I still use caution, as there is always the possibility of a government backdoor. That said, since I am not a programmer or developer, there is no way for me to know how well these applications work (if at all), except by reading through the technical whitepapers to see if all checks out to me as a layman, or, perhaps, by taking a look at market feedback.

For this section, I will grade the most popular encryption applications using the criteria of price, ease of use, and encryption capability. This includes, both, contract and no-contract plans (that is, if the "burner" phone is a smart phone). I will be testing various free applications on my iPhone. Results with Android phones may differ.

**1. Surespot**

Surespot is an encrypted messaging application, available on both the Apple Store and Google Play. For basic instant messaging, it is free of charge, but if you want to use the voice messaging function, you will have to pay $1.99.

Surespot uses end-to-end encryption, utilizing 256 bit AES-GCM keys created with 521 bit ECDH. Their website denotes that ECDH means that only you and the receiver are able to decrypt the messages. One other positive, is that there is no association with your phone number or email, which is not a feature with some other applications.

I have been using the Surespot application for a year and have had no issues, whatsoever. It's easy to setup, notifications are pushed, and it has *never* crashed on me. It's worth mentioning, that if you get a new phone, it is difficult to re-setup the account on the new device. That happened to me and I just opted into creating a new account.

In May 2015, an article revealed that 115 ISIS-linked operatives were found to have been using Surespot; if it functions well enough to facilitate terror attacks, it should work just fine for peaceful privacy advocates. That is, until the trial of Ali Shukri Amin, an ISIL sympathizer that used the application, concerns have been raised (Surespot was specifically named in the aforementioned linked Statement of Facts); specifically, there are fears of a potential backdoor, and some outlets have stopped promoting it.

Although, the Electronic Frontier Foundation (EFF) rated the application a 5 out of 7, with the downfalls being that past communications are not secure if your keys are stolen, and that there hasn't been any recent code audit.

**2. Signal**

Signal is probably the most popular encryption application for both Apple and Android users. It was designed by Open Whisper Systems, and comes with quite a few accolades. For one, Edward Snowden advises you to "*Use anything by Open Whisper Systems*." Additionally, Bruce Schneier, internationally renowned security technologist, asserts: "*I am regularly impressed with the thought and care put into both the security and the usability of this app. It's my first choice for an encrypted conversation.*"

Suffice it to say, the technological loadout is quite extensive, which leads me to believe that it might just be the most secure way to enjoy privacy on a smartphone:

- **Instant Messaging**
  - Signal uses Curve25519, AES-256, and HMAC-SHA256
  - Signal uses end-to-end encryption
  - Signal utilizes the Axolotl, the most advanced cryptographic ratchet available
    - Axolotl generates new AES keys for every single message
  - Signal improved upon the technology of Off The Record (OTR)
- **Phone Calls**

- Signal voice calls are encrypted with the RedPhone encryption protocol, based on the Zimmerman Real Time Protocol (ZRTP) and Secure Real Time Transport Protocol (SRTP).

I downloaded and setup the Signal application, and tested out the phone call and messaging function. It's extremely easy to download, setup, and use, although it does require you to verify your phone number and share your contact list. In summation, in EFF's secure messaging scoreboard, they gave Signal a perfect 7 out of 7.

**3. Telegram**

Telegram is a cloud-based encrypted messaging application available on iOS, Android, Windows Phone, and Ubuntu Touch. It is also available on the Windows, OS X, and Linux desktop systems. It is free for download and also has encrypted file transfer capabilities.

In the previous examples, I haven't mentioned anything about the companies or founders of the application, but this one is an interesting story. Telegram was launched in 2013 by brothers Nikolai and Pavel Durov. They had previously founded VK, a Russian social media network, but moved on to other projects when it was seized by the Russian Government. In one interview, Pavel expressed libertarian sentiments, and now travels from country to country every few weeks with a group of computer programmers.

So, how does Telegram work?

Like Signal, you will have to provide your phone number and verify it. It is not required that you sync your contacts list, but if you do, it alerts you when one of your contacts installs the application.

Telegram utilizes Nikolai's MTProto protocol, which uses AES-256 bit and RSA 2048 encryption, and also the Diffie-Hellman key exchange. One of the most intriguing features of this application is the secret chat function, which Telegram describes as such:

> *"Secret chats use end-to-end encryption. This means that all data is encrypted with a key that only you and the recipient know. There is no way for us or anybody else without direct access to your device to learn what content is being sent in those messages. We do not store your secret chats on our servers. We also do not keep any logs for messages in secret chats, so after a short period of time we no longer know who or when you messaged via secret chats. For the same reasons secret chats are not available in the cloud — you can only access those messages from the device they were sent to or from."*

You can also send encrypted files in secret chats:

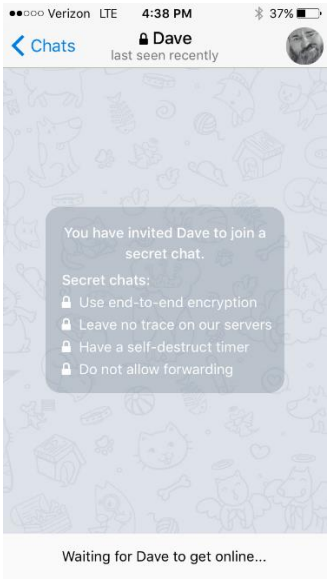
> *"When you send photos, videos or files via secret chats, before being uploaded each item is encrypted with a separate key, not known to the server. This key and the file's location are then encrypted again, this time with the secret chat's key — and sent to your recipient. He can then download and decipher the file. This means that the file is*

> *technically on one of Telegram's servers, but it looks like a piece of random indecipherable garbage to everyone except for you and the recipient."*

For group chats on the other hand, you can utilize the cloud chat feature. From what I can gather, those are still encrypted, but just not as strongly as the secret chats, which, as mentioned previously, use end-to-end encryption.

The final note worth mentioning in regards to the encryption scheme, is that after a key has been used 100 times or for more than a week, it is destroyed and replaced.

I actually downloaded and used this application today. I started a secret chat with Dave from the Seeds of Liberty podcast, and also joined their group chat. It was easy to install, setup, and initiate calls.




In summation, EFF gave them a 4 out of 7 with the downfalls being: the provider can read the messages, you cannot verify your colleague's identity, and past communications are not secure if your keys are stolen. Although, for the secret chat feature, they were given a 7 out of 7—I'd suggest that you consider utilizing that secret chat feature, friends.

**Anonymous Browsing?**

Not only are there privacy applications for messaging and phone calls, but there is also a way to browse the web anonymously using the Tor iOS browser. I'm not quite sure if it is available on other operating systems, but as I mentioned previously, I'm only concerned with what I am actually able to test.

The free application that I use is called "VPN Browser – Tor-powered free VPN for anonymous Internet browsing." You will download it, open it up, and it will connect to the Tor servers. Before you do anything, I'd recommend going to "Yahoo.com" or some site like that, to ensure you are using an anonymous proxy – that, or you can hit the "Settings" button, click the "Tor Panel," and it will show you your IP address and the location (if the location is known).

Please note that when you are using the Tor browser, the only information that is being protected is that of the browser – other information on your phone will still go through normal internet protocols, leaving them open for government snoops or hackers to access.

Why should you use the Tor browser? First off, it prevents websites and other services from learning your location, which can circumvent the tracking of your habits and interests. Secondly, it prevents people from watching your traffic locally. Lastly, Tor transmits your connection through multiple relays, making it much harder for any single relay to learn what you're up to.

Although, there are a couple of points of concern that I have with this application. It's quite buggy and there are advertisements in the free version, that take over the browser every five minutes or so. Other than the slight annoyance, it's all well and good, but the advertisements still bring up companies from Central Illinois, when my proxy is somewhere out in the Pacific. Does this mean that I'm still being geo-located despite using a proxy server? Uncomfortable thought, isn't it?

It should also be noted here, regarding Tor specifically, that it might very well have been compromised by now, but independent verification has not been done yet, to my knowledge. I say this because Ian Bernard's home was raided by the FBI last month, and Chris Cantwell made the following observation:

> *"Concerns about the security of the Tor network were raised in the wake of the trial of Ross Ulbricht, the creator of the Silk Road online drug market. It has been known for some time that an attack on the Tor network was at least theoretically possible, but this was thought to be time consuming and only useful for uncovering servers which were steadily connected to the network. Uncovering the identity of an individual who happens to be visiting a site at some point or another, is news at least to me."*

If this pans out to be true, then competitors to Tor just might surface to provide better onion-routing, like Tribler. Unfortunately, when it comes to digital encryption, the field is developing so dynamically it can feel at times like a full-time job just trying to keep track of what the current status of these new technologies are, besides the fact that there are just certain unknowns that must be investigated if libertarians are going to make fully informed decisions about the exercise of their right to privacy.

That said, there are multiple applications that promise Tor protection; this is just the free VPN browser that I have used in the past—there may be better options available for anyone interesting in further investigation.

**Conclusion**

The initial question that was to be answered was this: **Is it possible to browse the Internet and talk anonymously using telephones?**

The answer is "yes,"; it is possible to gain anonymity using payphones (if you can find one), you can purchase a prepaid phone (through multiple carriers) without providing any personally identifiable information, and you can also browse, talk, and message anonymously, while using encryption on smartphones.

As I mentioned previously, I would still proceed with caution when discussing any sensitive information, as it is hard to know if any of those encryption companies have been compromised; they probably aren't, but its better safe than sorry, at least until such time that independent computer programs are willingly able to provide audits that are published as white papers over the Internet. Additionally, the capabilities of the State to break through encryption is somewhat unknown, especially when considering the unknown, illegal process used to find the Silk Road server.

With all that said, I still highly encourage the use of encryption, just as the EU Parliament did in 2001:

> *"In contrast [to telephones], e-mails can and should be encrypted by everyone. The oft-repeated claim that a person has no secrets and thus has no need to encrypt messages must be countered by pointing out that written messages are not normally sent on postcards. However, an unencrypted e-mail is nothing other than a letter without an envelope. The encryption of e-mails is secure and relatively straightforward and user-friendly systems, such as PGP/GnuPG, are already available, even free of charge, to private individuals on the Internet. Unfortunately, they are not yet sufficiently widely distributed. The public authorities should set a good example and themselves employ encryption as a standard practice in order to demystify the process."*

Encryption is not guaranteed to work *every time*, but at the very least, it makes things much more difficult for the State. Just because your iPhone fails 2% of the time, doesn't therefore mean that you should stop using it—the same goes for encryption.

As is the trend with the State, this entity does not create anything of value; rather, it steals technology and innovations from the free market. There is no exception when it comes to the mass surveillance apparatus that most 21st century human beings have become accustomed to. One way to get ahead of the State, is with the mindset of crypto-anarchy, which is largely geared around privacy.

I'll conclude with a fantastic slogan from a shirt that I very much want to get:

> ***"Dance like no one's watching. Encrypt like everyone is."***