

Protecting From Spying Eyes On Your Metadata

Unless you've been living under a virtual rock, you've heard about the increasing concern over NSA's ability to monitor the digital information of American phone calls, emails, and text messages. It's the first amendment right granted by the Constitution to complain about what the government does.

However, before you start microwaving your hard drive or flushing your cell phone down the toilet in fear that a government agency will use that information against you, it's important to first get the facts straight.

What is Metadata?

Many of the headlines you'll read regarding this issue talk about the topic of metadata, a part of everyday communications most people don't think—or even know—about when sending digital files. When you send a letter, its delivered in two parts: the addressed envelope and the contents of the letter itself. The same applies to an email or text: you send the message itself attached to a deliverable address and, maybe, subject line.

Essentially, metadata is the part of the file that's needed for a message to arrive at its destination. The addressed envelope, email address and subject line, Twitter hashtag, and phone number are all forms of metadata. This differs from the message, or data, itself, especially as far as the NSA is concerned.

Everything said inside the envelope, in the body of an email, over a phone call, or on a Facebook post is the message attached to the metadata. In laymen's terms, if you shout someone's name across a room to get their attention, the name

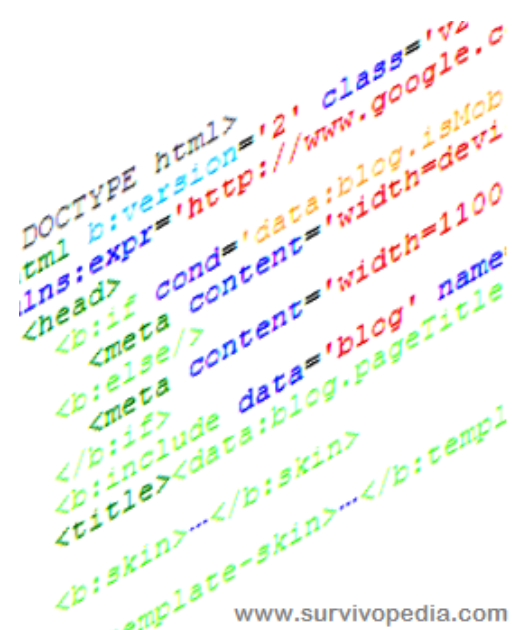
shout is the metadata. Whatever you say to them after you've made contact is the message.

Though the dividing line between the message and the metadata may seem arbitrary, it creates a problem within American law.

Due to the first amendment, privacy, and intellectual property laws, the message is typically protected by law against infringement from spying eyes. Unfortunately, the law is yet to recognize the attached metadata as warranting the same protection, even though programmers often require the input of sensitive material into the metadata.

Metadata and Your Privacy

This creates a problem when you get a situation like the Verizon court order, where it was unveiled that the NSA was collecting the phone records of millions of US users. This required Verizon, one of the largest telecommunications providers in the US, to hand over the numbers of both parties on each call, location data of the phones, call duration, and time of calls.



```
DOCTYPE html>
html b:version='2' class='v'
<ins:expr='http://www.google.c
<head>
  <b:if cond='data:blog.isMob
  <meta content='width=device
  <b:else/>
  <meta content='width=1100
  </b:if>
  <b:include data='blog' name=
  <title><data:blog.pageTitle
  <b:skin>...</b:skin>
  <template-skin>...</b:templ
```

www.survivopedia.com

In other words, they were to hand over the metadata of millions of Verizon subscribers. This may draw up the obvious question of why Verizon seeks to track this user data in the first place; and the answer seems simple. Cell phone companies aren't seeking to track your whereabouts or digital doings for reasons of surveillance. They do it so they can understand how cell phones work and interact and how cell towers track and transmit calls.

Furthermore, in order to continually enhance and maintain

service and attract new users—partly to create those dotted color maps representing coverage across the country—the telecom companies need to track where their users are and how they move around.

For phone company purposes—the same of which apply to Facebook, Twitter, Gmail, and so on—knowing your metadata helps keep the service up and running. These companies seems to have little interest in your personal life and information, aside from knowing your interests to further bolster advertisement streams.

However, apart from not using or carrying a phone or computer, there isn't much you can do about keeping that information secret from your mobile phone company or Internet service.

However, the world did learn about the PRISM program thanks to one of Edward Snowden's many Wikileaks slides. The program unveiled that some of the biggest media and communications companies in the world, among them Microsoft, Google, Yahoo, Facebook, YouTube, Skype, and Apple, were in cahoots with the NSA to provide them with user email, video chats, photos, stored data, file transfers, login activity, and social networking details if requested.

Here's the bad news: if you don't want to have the NSA to have any chance of spying on your activities on these programs, your only option is avoid using them. That's not to say that you should stop using Facebook and Gmail right now, but you should if you are absolutely desperate to keep your information away from the NSA.

Unfortunately, these aren't the only companies involved in PRISM, nor does there seem to be an end as to how many could come under its umbrella.

Protecting Your Metadata



Fortunately, there are some things you can do to [keep your metadata secure and private](#). Doing so may not only keep the government's prying eyes out of your personal life, but also any other unwanted individuals who may want to steal your identity or take advantage of your private data.

On computers and smartphones, which are basically handheld computers, the main means of protecting your personal information, both message and metadata, is through cryptography. In its simplest terms, cryptography is a way of using a mathematic algorithm to rewrite information in a secret code.

In digital communication, cryptography uses the exchange of coded keys, or long strings of numbers that each party uses to encode and decode each other's messages. Like any other form of computer programming, cryptography comes in a variety of languages, including the Diffie-Hellman key exchange, public-key cryptography, and symmetric key exchange.

You don't necessarily know how to "speak" these languages, as they are most often left up to mathematic functions that are easy for computers to create.

However, these functions are very difficult to undo, so much so that even the NSA can have difficulties circumventing some

key exchange crypto codes.

The most viable and effective forms of cryptography comes in the form of end-to-end encryption. Unlike most forms of encryption, not even the server a message passes through can look at your messages this way. The server may still pass on the associated metadata to a third party, but will only see encrypted code as the message. The catch: end-to-end encryption can be difficult to use and may only be worth exploring if you're passing along extremely sensitive information.

Fortunately, servers like Google already optimize their security efforts by using a code known as SSL to hide your information from third parties, though they pick up your metadata in the process. This is something you can't avoid. Google will always have your metadata, as they need it to keep the network working. But without taking advantage of Google's SSL, your metadata gets transmitted unencrypted.

In the meantime, there are tools that exist to help hide the content of things like email messages from any possible prying eyes.

One, called Pretty Good Privacy (PGP), offers a way for two parties to use peer-to-peer encryption so that only the sender can encode the message and only the receiver can decode it. PGP can currently be purchased by Symantec, but offshoot programs are also available and can still be created by savvy programmers.

With these types of programs you can feel safe that your messages will pass through the web worry-free, but there is no guarantee they'll be safe from the NSA.

Such is the underlying theme of this issue. There are many different tools and precautions you can use to protect yourself when using the phone and Internet, but in the end no form is 100% effective.

Just like sex, drugs, and alcohol, the only way to truly protect yourself from the potential dangers are to abstain completely.

How to Shield Yourself From the Government's Peeping Tom Camera

WATCH VIDEO



*This article has been written by **Cody Griffin** for [Survivopedia](#).*