THE BONNER-DENNING LETTER

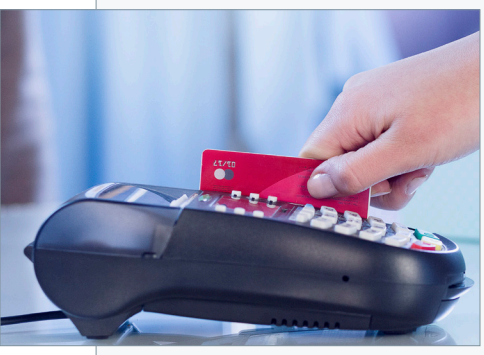
ONLINE PRIVACY GUIDE

BONNER & PARTNERS

The Bonner-Denning Letter

SPECIAL REPORT 2018

CONTENTS



Online Privacy Guide

By Nick Rokke

Federal agents led Leigh Van Bryan to an airplane. After hours of questioning and more than twelve hours in a holding cell with two Mexican drug dealers, Leigh was denied entry to the U.S.

Leigh and his friend Emily Bunting were about to go on their first American holiday. The British duo had never been to the States and were looking forward to seeing Hollywood.

Unfortunately, a couple of Leigh's excitable tweets got him flagged by the Department of Homeland Security. Earlier in the week, he tweeted to a friend, "Free this week for a quick gossip/prep before I go and destroy America?" This may sound incriminating, but any of Leigh's British friends would have understood "destroy" was slang for getting drunk and partying.

That tweet and another one about "diggin' Marilyn Monroe up" (a quote from the satire cartoon *Family Guy*) got him flagged.

It's About More Than Big Brother

Government agencies use digital surveillance of web communications to follow foreign terrorist suspects. This is a noble cause – we need to know if there is a threat of attack by terrorists. But as Bill explains in his book, *Hormegeddon*, what starts as a beneficial program can quickly morph into something completely different.

The National Security Agency (NSA) has the authority to listen in to billions of mobile phone calls made every day around the world. They have the ability to transcribe and quickly search these calls for key words or phrases.

And calls made by foreigners aren't the only ones they monitor. The NSA also listens in to and records calls by American citizens.

In addition to monitoring phone calls, the organization also keeps a record of all the texts and emails it can get its hands on. To help with that, some government agencies, including the NSA, ask companies to create a backdoor for them to access the info. Most companies comply with this request.

But that causes a problem – if there is a backdoor for the government to get in, it can also be accessed by others. You might not be scared of the government monitoring you, but you should be concerned about what hackers can do to you.

If a hacker just steals your identity and maxes out a few credit cards, you're lucky. This will "only" cost you, on average, $1,500 and 30 hours of your time to legally get the erroneous charges expunged from your record. That's a relatively quick fix.

But be warned, if someone gets into your bank account because of something you did (or didn't do), your bank may not be obliged to reimburse you.

If the bank's systems leaked the data, you're covered. However, if the criminals get in through your systems, you may not be reimbursed for any losses suffered. For instance, one Seattle man had $12,000 taken from his account by scammers. A small construction company lost $545,000. In both cases, their bank refused to reimburse them because the electronic devices on which their online banking was set up were not secure.

But financial losses may not be the worst of your problems. It is possible to be stalked and blackmailed through your personal, everyday electronic devices. If you have GPS in your phone, there are ways for people to follow you. And it is possible for someone to remotely activate the video recorder on your cell phone or laptop and record you doing potentially embarrassing acts. One Canadian girl had a topless video of her posted on the Internet by a stalker. The embarrassment and bullying she endured at multiple schools as a result allegedly caused her to commit suicide two years later, when she was just 15.

Privacy may be harder and harder to achieve, but it is more important now than ever. In this report, we show you several ways to protect your privacy and keep your personal data secure.

How to Surf the Web Privately

There are many different ways to protect yourself from potential privacy breaches while surfing the web. When it comes to private web surfing, we break the term "privacy" into three different categories:

1) Privacy from people using your computer

Most people have a computer or laptop at home that is used by all the family. Why would you want to maintain privacy on your home/personal computer, laptop, or tablet? A couple of reasons.

First, let's say you want to buy something for your wife or kids as a surprise. You don't want them to see that you've been checking out a certain site – it would spoil the surprise. Or you want to make sure thieves find no sensitive data – such as your credit card details - if they steal your laptop. Here are a few simple steps you can take.

a) Use a private window. The easiest way to hide your browsing history (a log of all the webpages you have viewed) is to launch a "private window." In Google Chrome, it's called an "incognito window." These windows do not record your browsing history or save cookies or other kinds of trackers.

What is a cookie? It's a small file a website saves to your computer signaling that you've been to its site. Most of the time, cookies are helpful. For instance, a cookie will keep you logged in to a site so you don't have to enter your password every time you go to access it. But some cookies save sensitive data like your username and address. If you are serious about your privacy, you should never allow your web browser to save your password.

Some cookies track your movements on the web. This allows advertisers (or criminals) to track your interests and build a profile on you without your consent. Have you ever noticed an ad on Facebook for a website you recently visited or a hotel you recently searched online for? If you have noticed this, you have a tracking cookie.

b) Clear your browsing history. If you forgot to launch an incognito web browser, deleting your browsing history (also known as clearing your cache) and cookies is easy. In your browser settings (or options), you should see a button to clear the history. Click that. Then look for a button to delete cookies.

There are too many different web browsers for us to give step-by-step instructions for each. A simple Google search should bring up several easy-to-follow tutorials.

Remember, this is just to remove the data from your computer. This will not remove data other people have already collected. For instance, if you use a Google incognito window to check your Gmail account and stay logged in, Google will continue tracking you if you watch YouTube videos… even if you are still in an incognito window. If you have some friends over and search YouTube for a video of last night's knockout punch or winning touchdown, you'll see YouTube suggestions based on your recent viewing history. If those results show *Keeping Up with the Kardashians* and *Project Runway*, merciless teasing will ensue.

2) Privacy from marketers

Certain websites track your activity no matter what. Facebook uses everything you and your friends post to help advertisers target you. Google tracks every search to help improve the experience for future users (and future advertisers).

So, how can you get around this?

Deleting cookies and trackers is a good start when it comes to maintaining privacy from marketers. But there are ways to stop them even before they plant cookies on your computer.

a) Avoid sites that track your activity. Easier said than done, right? Almost everybody has a Facebook account these days. But if you want to continue using sites such as Facebook, you need to be aware of everything you or your friends post to your wall. Don't post that you're leaving on a two-week European vacation. You may be publicly inviting burglars to stop by.

b) Use a different search engine. Instead of using Google for searches, you can route your search through StartPage. This site routes your searches to Google, but through its own servers. That way, Google won't know who sent the search. Or you can get more privacy from a search engine such as DuckDuckGo. This site doesn't track searches at all.

c) Use a browser extension service. Another way to avoid cookies and trackers is to install a "browser extension" like Ghostery or Privacy Badger on your web browser. To do this, you can go to either website and follow the instructions to install the program. Apps like these allow you to control what kind of cookies or trackers reach your computer.

There are trade-offs for maintaining your privacy. Most people still use Google because they are not doing anything that they care if Google sees. And Google is known for giving great search results. Some argue that Google and Facebook make life easier.

So, if you decide you want to continue using these popular sites/apps because you like them, or they help you in any way, just be aware of the dangers and act accordingly.

3) Privacy from hackers

Keeping hackers from your data is the most difficult to accomplish. Doing all the above will help, but it's not enough.

You need to be proactive at all times against this threat. You never know when someone is going to be watching what you type or send over the web. Here are some simple ways to protect your data from hackers while online.

a) Avoid public Wi-Fi. The No. 1 thing you can do to keep hackers away from your data is to never log in to any website while on free Wi-Fi. Hackers can set up what's called a "man-in-the-middle attack" and steal your username and password as soon as you click send.

Some people think if they're on a secure website, they're safe. Most websites begin with "http." You'll know if you are on a secure website if the web address begins with "https." You also will see a picture of a latched padlock next to the web address.

But these secure websites only ensure your data is safe once it gets to the host site. A man-in-the-middle attack can intercept your login details before they even get there.

Luckily, there are steps you can take to secure your device if you like using public Wi-Fi:

(i) Mobile hotspot. The easiest thing to do is to set up your phone as a mobile hotspot. This process is called "tethering." Most phones let you do this.

Check with your wireless carrier for instructions on how to set up tethering on your phone.

Once you set up a hotspot, you can connect your computer, laptop, or tablet the same way you'd connect to any other Wi-Fi network.

If you create a hotspot, make sure you password-protect it. Otherwise, your hotspot will be just like public Wi-Fi and you'll have the same problems.

And never log in to someone else's hotspot unless you know who it is – it could be a hacker trying to get your data.

(ii) Install a Virtual Private Network (VPN). Another protective measure to take when using public Wi-Fi is to install a Virtual Private Network (VPN) on your computer. A VPN is a program that directs all your internet traffic through its server instead of public Wi-Fi. After you install a VPN, you simply launch the program any time you connect your device to public Wi-Fi.

One feature you should look for in a VPN is "end-to-end encryption." Encrypting your data is important. And for your data to remain encrypted, the data must leave your computer encrypted and stay that way until it reaches the VPN servers. This way, if a hacker is watching you, he will be able to tell you are sending data, but unless he has the encryption key, he won't be able to decipher what you sent. But if the data isn't encrypted on both ends, hackers will be able to read your data.

We don't recommend any specific VPN providers. But for a detailed review of several VPNs, just click here.

b) Use different passwords. Using the same password for every site will make things a lot worse if you are targeted by a hacker. A hacker could access all your accounts if your password is always the same. So, it is important to change your password for different sites.

You can either come up with a system to create new passwords, or get a password management app like LastPass or Dashlane.

Private Email, Texts, and Calls

Keeping emails and text messages private is just as important as keeping your web browsing private. In fact, you can follow many of the same precautions to ensure your messages are secure.

1) Email privacy

Today, we share many of our most private details with others through cyberspace. Whether it's personal transactions, business deals, or love letters, they are all turned into ones and zeroes and sent into the digital abyss. These messages go through servers, nodes, and cables to their destinations. That gives people plenty of opportunities to intercept your message. So here are a few things you can do to prevent that:

a) Encrypt your emails. As with encrypted browsing, both you and your message's recipient need to have encryption. If one of you does not partake in the encryption, the message is not secure. So, if you are serious about email encryption, you will have to get others onboard.

Many people use PGP encryption. This is a free service with strong encryption. Most hackers will not be able to break the encryption. Neither will the NSA, if your encryption key is good enough.

You can install apps on your computer to encrypt emails from desktop programs (think Outlook) and from web-based email clients (Gmail or Hotmail).

For details on how to do this, check out this article on Lifehacker.

b) Avoid free email service providers. Another important factor when it comes to the privacy of your emails is the service you use. Do you use a free email provider like Microsoft, Yahoo, or Google? Be assured, there are no free things in life and email is no exception. These companies all use the emails you send to collect information to help marketers target you.

While using your web-based email, have you ever noticed an advertisement on the side suspiciously close to the topic of your email? You might now. If you type the word "baby" into an email – even if you're just sweet-talking your spouse – you'll probably see diaper ads. Writing about a trip to Vegas? You're probably about to be bombarded with ads from casinos.

If this kind of thing bothers you, you may want to consider paying for your email service. ProtonMail is one such paid email provider. Right now, you can even get a free secure email account from them. If you need more storage than the free account provides, there are options to upgrade. Another paid service is Neomailbox. It is more expensive than ProtonMail, but it has more options for maintaining privacy.

c) Use a non-U.S. email service provider. While on the topic of secure email providers, you should consider one hosted outside of the United States. This is just one more measure to protect yourself against a prying government. Both ProtonMail and Neomailbox have servers in Switzerland – where the government still considers privacy a basic human right.

Paid and non-U.S. email service providers are better options than most anonymous email websites. Anonymous email sites say you can send an email to someone without them knowing who sent it. Which is true – you can send an email and the recipient won't know who it is unless you identify yourself. The problem is most of these sites record your IP address. So, if you send this from your home, it's possible to trace who sent it. One example of an anonymous email site is

Send Anonymous Email – it lets you send messages, but records IP addresses… and has worked with the authorities. So, don't use this site if you want complete privacy.

2) Texting Privacy

Many people choose text messaging for communication instead of email. Texting creates a completely new set of issues.

First, let's talk briefly about simple phone security.

a) Always lock your phone. Some people like the convenience of not having to unlock their phone every time they want to use it. This is a mistake. In the best-case scenario, a phone thief only wipes all your data from the hard drive and sells your phone. Worst-case scenario: they log into all your apps, get sensitive data, and use that to steal your identity. Or someone could read your text messages and find potentially embarrassing information.

b) Be careful what you send. With texts (and emails), when you send them, you lose control of the text. Your recipient can get that message and save it forever. Everything you say can be used against you… forever. This doesn't just include the messages you send, but also any pictures and files you send through the texting app.

If you think you can get around that by using SnapChat – an app where you can decide for how long people can see your message – you're wrong. SnapChat stores the pictures and videos on its servers. This allowed hackers to release 100,000 "private" photos and videos in 2014, many of them of a very personal nature.

Outspoken tech billionaire Mark Cuban has a solution to this problem – an app called Cyber Dust. This app has all the same features as SnapChat, but it doesn't store files on its servers. Therefore, once the message deletes from the other phones, it is gone forever. Many businesses utilize this service to ensure privacy.

Mark Cuban created this app after the SEC investigated him for insider trading. Cuban watched as the SEC tried to use any message in any context they wanted to further their case. In the end, the courts found him innocent. But Cuban had to spend more money defending himself than if he had just paid the SEC fine. He was outraged and wanted to help others avoid a similar situation.

c) Encrypt your texts. Text messages sent from one Apple iPhone to another are automatically encrypted. That – along with other privacy measures – makes the iPhone a decent starting point for private messaging. We know the encryption is good because not even FBI experts can break into an iPhone. In a recent high-profile case, the FBI reportedly had to pay a company $1.3 million to unlock the iPhone of a suspected mass shooter after Apple refused to unlock it for them. But Apple immediately set about fixing the code to prevent that method of breaking into the phone. This is good for your security. Even if you're not doing anything illegal, knowing your phone is almost "unhackable" means criminals also can't break into your phone.

There are other apps available for private texting such as Privatext, Smiley Private Texting, and Private Space. These apps just encrypt your texts, but don't automatically delete your text like Cyber Dust does.

3) Phone Call Privacy

Ever since the Edward Snowden leaks in 2013, we've known that the NSA has the ability to monitor all of our phone calls. Taking that one step further means the technology is out there for anyone to listen in to your calls.

Think about the different parties you give personal information out to over the phone. Doctors, banks, credit card verification, the list goes on.

As far as you know, no one has illegally gotten your private info from your phone calls. But as most phone calls are now transmitted digitally, phone call encryption is now something you really need to think about. Here are a few things you can consider doing:

a) Use an encryption app. The quickest thing to do is install a call encryption app on your phone. Both Apple and Android phones have these kinds of apps. A quick Google search will bring you to services such as Ostel, Secure Call, and Cellcrypt. This list is neither exhaustive nor a recommendation, merely a starting point.

Be careful with the pricing for these apps. Some of the apps say they are free, but you can only receive calls from other people using the app. If you want to make a call, you will have to pay extra. Sometimes, a lot extra.

Keep in mind, for the call to be fully encrypted, both people need to have the encryption service installed. So, if you want your friends to be able to accept your encrypted calls, you might want to use an app that gives them a free download.

One encryption company mentioned frequently in the likes of *PC Magazine* and *International Business Times* is Silent Circle. This company has an all-around encryption service. You can download a Silent Circle app called "Silent Phone" to your phone. This app will get you started with phone call encryption.

b) Avoid public pay phones. These can be a great way to hide your identity from your caller. But beware, they're not a great way to maintain your privacy if you're giving any personal information. Just think how many people have had the opportunity to place a bug in the phone waiting for someone to leak their social security number while on a call.

c) Use a prepaid phone. A prepaid cell phone is another option. In movies, you often hear these called "burner" phones. That's because once you use the phone for your purpose, you throw it out so no one can trace you. But the NSA still has the technology to listen in on your calls if they can figure out the burner phone is yours. So, if you're worried about that, don't say anything that can identify you – unless you encrypt everything.

One last thing: Check your app permissions. Leaking data is a bigger problem than you might imagine. Free apps on your phone are one of the biggest culprits. Do you have a flashlight app on your phone? Chances are this app has permission to track your browsing history, phone contacts, and maybe even what you type. To stop this, look up how to check permissions on your app and adjust for maximum security. If you can't change the permissions, delete the app immediately.

How to Keep Your Payments Private and Secure

The end goal for many hackers is to get your payment information so that they can sell it to those who wish to misuse it. Credit card numbers sell for $10–$25 in the criminal underworld. One popular site, AlphaBay, often has over $200 million worth of credit card information on it at any one time.

Our resident technology expert, Jeff Brown, put it like this:

I can buy your credit card number for $10… right now.

In fact, any cybercriminal could buy your card number, your security code, your PayPal or eBay username and password, all of your health records, and your bank account details… for a total of just $69. They just have to know where to go.

The Internet isn't all that it appears to be.

Search engines like Google or Yahoo compile and index gobs of information. But they show you just 0.03% of the information that exists on the World Wide Web. Ordinary search engines cannot access the 99.97% of the Internet that makes up the "Deep Web."

This may sound unbelievable, but just think of all the webpages that require a password for access. Google and Yahoo can't show you those. But that's not what you should be concerned about.

The real danger is what's hidden within the Deep Web. This is where the "Dark Net" exists. And it's where much of the criminal world conducts its business.

Using special software and web browsers, anyone can go to one of the dozens of "Dark Market" sites – places with names like Silk Road, Cloud Nine, Pablo Escobar Drugstore, Hydra, or Zero Squad – to buy and sell guns, sex, drugs, counterfeit goods, and your stolen credit card information. They can do it just as easily as you'd buy a used iPhone on eBay.

And business is thriving.

With most payments being processed electronically (think debit and credit cards), our transactions are recorded digitally in many places.

Let's say you stop at the store to buy a pack of gum. You have no cash so you put it on your credit card. The store needs to send this information to its payment company – either a merchant account at its bank or a payment processing company like Square. From there, your payment info goes to your credit card company (e.g. Visa or MasterCard). Then your payment is passed along to the financial institution that issued you the credit card (e.g. Citibank or JPMorgan Chase).

Did you follow that? At least four different companies have to see your payment information before the transaction is complete. Plenty of opportunities for a hacker or government organization to see what you've purchased and get your payment details.

Hackers have managed to breach databases at all levels of transactions. Many people who shopped at Target in 2013 and Home Depot in 2014 were victims of data breaches. Heartland Payment Systems – one of the world's largest payment processors – was hacked between 2006 and 2008. Hackers compromised JP Morgan Chase's systems in 2014. Just these four hacks alone exposed over a quarter of a *billion* records.

To protect against getting your credit card or bank information stolen, you have to be very careful. The most foolproof protection measure is to be old-fashioned. Use cash. By using cash, your info won't be stored on

merchants' networks. Hackers can't get your financial information if it isn't recorded.

Cash also has the benefit of keeping your purchases secret. No one or no agency will be able to track your purchases if you use cash.

But you can only use cash in the physical world. Mailing cash for an online purchase is a bad idea. Here are three different measures you can take to protect your payment privacy on the web.

a) Use gift cards. By using a gift or prepaid card, you have a unique card number for every new gift card. This way, even if someone gets the number, the amount you stand to lose is limited to the amount on the card balance. But this will not work if you use a "reloadable" card and keep the same card for a long time.

Gift cards are anonymous. Your name isn't attached to it. To ensure your privacy, buy the card with cash from a retailer. Then it will be almost impossible to track it back to you. But be aware that if you order a physical item using the gift card and get it shipped to your home address, you lose that anonymity.

b) Use a virtual credit card. Every major credit card issuer will allow you to set up a virtual card. If you sign up, you will get a unique card number to type in for virtual purchases. You can change the number whenever you want – we recommend doing so at least once every three months. That way, if the information gets out, the hackers will only have a stale number.

c) Use a privacy service. Abine is a full-scale privacy service. It comes in a free version and a premium (paid) version. The free version will help you set up unique passwords at different sites and encrypt messages. With the premium version, you can set up a "Masked card." This is a lot like a virtual credit card. But you fund this card immediately before the purchase (with the exact amount needed for the purchase). That means if this card number gets out, no one could charge to this card because there would be no credit available. Also, you can change this number as often as you like.

What about Bitcoin? You may have noticed we did not mention the cryptocurrency Bitcoin as a good privacy measure. This was intentional. We don't believe Bitcoin is a good way to maintain privacy.

First, your Bitcoin wallet is digital, therefore it can be hacked. So, you don't want to leave a large balance in your wallet… even if you are okay with the volatility of the price of Bitcoin.

Second, all Bitcoin transactions are recorded on the blockchain. So, your history of owning bitcoins and where you sent the bitcoins are a matter of public record. Bitcoin is not anonymous.

HOW TO ESTABLISH ONLINE PRIVACY

BY NICK ROKKE

USE A PRIVATE WINDOW

The easiest way to hide your browsing history (a log of all the webpages you have viewed) is to launch a "private window." In Google Chrome, it's called an "incognito window." These windows do not record your browsing history or save cookies or other kinds of trackers. If you are serious about your privacy, you should never allow your web browser to save your password.

WHAT IS A COOKIE?

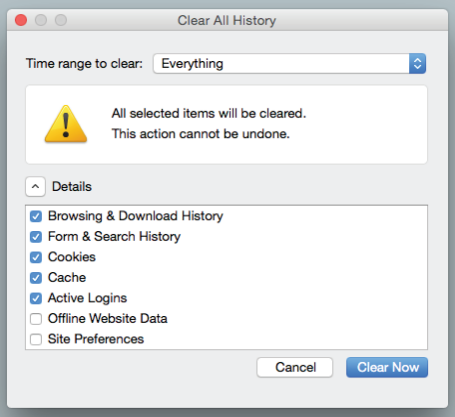
It's a small file a website saves to your computer signaling that you have been to the site. Most of the time, cookies are helpful.

CLEAR YOUR BROWSING HISTORY

If you forgot to launch an incognito web browser, deleting your browsing history (also known as clearing your cache) and cookies is easy. In your browser settings (or options), you should see a button to clear the history. Click that. Then look for a button to delete cookies. Remember, this is just to remove the data from your computer.

STEP-BY-STEP INSTRUCTIONS

There are too many different browsers for us to give instructions for each, but a Google search should bring up several easy tutorials.



UTILIZE MOBILE HOTSPOT

The easiest thing to do is set up your phone as a mobile hotspot. This process is called "tethering." Most phones let you do this. Check with your wireless carrier for instructions on how to set up tethering on your phone. Once you set up a hot spot, you can connect your computer, laptop, or tablet the same way you'd connect to any other Wi-Fi network.

PASSWORD-PROTECT ACCESS TO YOUR HOTSPOT

And never log into someone else's hotspot unless you know who it is – it could be a hacker trying to get your data.