Encryption, Privacy and the Dark Side of the Internet

By Duane Croft

The Internet is now a part of our daily lives. Almost everyone uses it, almost every day. Most people with smartphones have Internet access 24 hours a day. However, I am not certain if most people realize how less than secure anything they do on the Internet is. Unless a person takes specific actions to prevent it, almost **anything** you do on the Internet can be observed by other people.

For example, you decide you want to write an email to your brother Bob. You write the email, input his email address and click "send," and it goes straight to him. Except it doesn't. It goes from your computer to your mail server. Your mail server reads Bob's address and sends it to another server. This server reads the address and sends it to another server. The email may bounce between 10 or more servers before it reaches Bob. And each and every one of those servers may keep a copy of that email. And anyone with access to those servers can read your email. (If you want to see some possible email routes, go to www.yougetsignal.com/tools/visual-tracert and run some proxy traces to a given server. If you choose mail.ou.edu, it will simulate some possible routes an email going to someone at the University of Oklahoma might take.) Recently there was a very high-profile scandal involving ex-CIA Director David Petraeus, where his extramarital affair was uncovered when an investigation turned up emails between him and his mistress. He thought his emails were private, that only he and his girlfriend could see them. He was wrong and it cost him his career and his marriage.

There are similar problems when you surf the Web. When you log on, your computer is given an Internet address (IP address). Every place you go on the Web records your IP address. You're on Facebook and see a link to the latest song by Lady Gaga that someone illegally uploaded. You click on it and download the song to your MP3 player. Six months later, the music industry can do a search and see what IP addresses downloaded the song and then send you a little letter saying if you don't pay them umpteen bucks, they will be filing a lawsuit against you. On the Internet, you have no privacy.

So the question becomes, is there any way to continue to use the net and have some level of privacy? This is particularly important for lawyers who are trying to communicate confidentially with their clients. And there is a solution, or at least a partial solution: encryption. I am going to talk about three different types of encryption ranging from the very easy to the somewhat more complicated. Encryption can protect your email from being read by anyone but the intended recipient. Encryption can prevent anyone from seeing where you browse on the Web. And while this sounds like a good thing, I will also mention some surprisingly bad things that have resulted from this.

LEVEL ONE: AES — 'ADVANCED ENCRYPTION STANDARD'

AES is really simple encryption that is easy enough to use with most clients. It is a built-in capability for PDF files. It is very easy to encrypt a file this way and all you need is the password in order to decrypt the file. This makes it nearly perfect for sending secure emails. It is not the most secure encryption available, but if you use the higher level settings and pick a strong password, the security level should be about the same as a typical banking transaction. However, if you use a lower level setting and/or a simple password (e.g. "123456" or "password"), there are lots of programs available that can crack this encryption.

How to use AES to encrypt a PDF file: Let's say you've prepared a confidential document and want to send it to your client via email. If you're using Windows, you'll need programs like MS Word and Acrobat. Open the document in Word. Click on the Create PDF in the Acrobat Ribbon — this creates a PDF version of your document. Then open the PDF in Acrobat. Click on File, then Document Security. Select Standard Security and choose a user password. Choose the highest encryption level available for your version of Acrobat — 128 bit or higher is preferred. 128-bit encryption is the minimum level of encryption used by most banks for encrypting electronic transactions. This will produce an encrypted PDF file that you can safely email to a client. When the client, or anyone else, attempts to open the PDF file, a pop-up box will come up asking for the password. If the correct password is entered, the PDF opens like normal. There are many other ways to do this. I'm a big fan of Open Office. Using Open Office, open your document, then select File, Export as PDF, then select the Security tab on the PDF Options pop-up and enter your password. This will also create an encrypted PDF file, just like the above.

The above process creates an encrypted file that will stop most people from being able to read your confidential material. Can the encryption be broken, say by people with supercomputers? The National Security Agency, as recently as April 2012, denies being able to break AES encryption.[1]

LEVEL TWO: PGP – 'PRETTY GOOD PRIVACY'

PGP is more complicated to use, but provides much higher security. There's also a variation of it called GPG, which is used primarily in Linux. Commercial and free versions are both available; the commercial versions give you some additional capabilities (such as encrypting all or part of your hard drive). It is a little harder to use because if you want to send a PGP encrypted file to someone, they have to have PGP (or GPG) also in order to open it. You can download commercial versions of PGP from Symantec at www.pgp.com.

PGP is a two-key system. After you install PGP, the first thing you have to do is generate your personal keys. You tell the program what email address (or addresses) the keys are going to be linked to and what password or pass phrase you will use. It will then generate two keys: a public key and a private key. You never give out your private key or your pass phrase to anyone, but you can give out your public key to the world. PGP will even (if you request) publish your public key to key servers on the Internet, so that people can search for you by name or email address and download your public key. It's also a good idea to keep a backup of your private key somewhere, because if you lose it (via a computer crash for instance), you'll never be able to decrypt your PGP files again.

After this, it is fairly simple to use. Say you want to send a private email to your brother Bob. Bob needs to have PGP and you need to have a copy of Bob's public key. Prepare a file you want to send him. Then tell PGP to encrypt the file — if you're using Symantec's PGP, you open their desktop and point and click on the file name and choose the encrypt option. PGP will ask whom to encrypt it for and give you a list of what public keys you have. Pick Bob's key and PGP will produce an encrypted file — it's actually a text file and will look like garbage. Email the file to Bob. When he gets it, he will ask PGP to decrypt it. PGP will ask for his password or pass phrase and then decrypt the file using Bob's private key.

There are some other options with PGP. Some of the commercial programs, including Symantec's, can produce self-decrypting archives (SDAs). These are files that have the decryption program built into them, so all that is needed to open them is a password. If you mail an SDA to someone, they do not need to

have PGP on their machine to open the file. However, they do have to be running the same operating system as you — if you're running Windows and they're running Mac, they won't be able to open the file.

Another very useful option available in both the commercial and non-commercial versions of PGP is "signing" a file. You can sign an encrypted file or a non-encrypted file. What signing a file does is add a bit of code to it, embedding information about the file and about your private key. Then anyone with your public key (and remember, you can give your "public" key to the world) can have PGP verify two things about the file: 1) that you (or someone with access to your private key and your password so it should only be you) actually sent the file and 2) that the file has not been changed since you sent it. So for instance, I can write up a confidential document, encrypt it **and** sign it with PGP and email it to you. When you open it with PGP, you will get a message from PGP about whether my signature is valid or not. If the signature is valid, you can have a very high level of confidence that I actually sent it and that no one has altered it since I sent it. This is a much higher level of confidence than you would (or at least should) have that a typed letter on paper with my written signature on the bottom is genuine.

There is one other big advantage of PGP encryption: It can provide much higher security. With AES encryption, we were talking 128-bit encryption. PGP will encrypt to more than 4000 bits of encryption. Every time you increase the encryption level by one bit, you increase the effort needed to break the encryption by a factor of 10. Going from 128-bit encryption to 4000-bit encryption is an astronomical increase in security. How good is this higher security? Well, in 2000, the FBI was investigating Nicodemo Scarfo, who was charged with racketeering, illegal gambling and loan sharking.[2] Nicodemo regularly encrypted his emails with PGP. The FBI could not break the encryption and had to resort to trickery. They got a search warrant for his house and during the search made a copy of his private key and installed a keystroke logger on his computer in order to get his password. That was 12 years ago. Can the FBI break PGP encryption now? I don't know. There have been numerous incidents reported in the press since then that indicate the FBI still cannot break PGP encryption, but none are as well documented as the Nicodemo Scarfo case.

"For the truly paranoid, remailers can be nested: send an encrypted email to ABC remailer with instructions to send the email on to XYZ remailer..."

As an aside, if you want more email privacy than simple encryption, you can combine PGP encryption with remailers. A remailer is a site where you send an email and it re-mails it to whomever you ask it to. For instance, you want to send an email to Bob again. You write your email and send it to ABC remailer. ABC opens it, sees the instructions you included for them to send it on to Bob and they do so. If ABC is a Type I remailer (also called a "cypherpunk" remailer), it can handle PGP. In this case, you could encrypt your original email for ABC before sending it to them. After they get it, they would decrypt it, see the instructions for sending on to Bob and then send the decrypted email onward. As additional security, most Type I remailers include some random latency period: after they get your original email, they hold onto it for some period, could be seconds, could be hours, before sending it on to Bob. This combats traffic analysis. Traffic analysis would be someone monitoring your ISP and Bob's ISP and seeing that every time you sent an encrypted email to ABC, that Bob gets an email from ABC seconds later. For the truly paranoid, remailers can be nested: send an encrypted email to ABC remailer with instructions to send the email on to XYZ remailer with instructions to send it next to PQR remailer and so on, with each of the intermediate emails encrypted. The final email to Bob can also be encrypted. You can go to www.email.about.com/od/anonymousemail/qt/How-To-Find-A-Remailer-To-Send-Your-Anonymous-Email.htm for more information about how to find remailers and how to use them.

LEVEL THREE: TOR – THE ONION ROUTER

PGP was the gold standard of privacy back in the 1990s. Then the U.S. Navy made all this obsolete and invented onion routing (which they patented under U.S. patent 6266704). In 2004, TOR was developed, which stands for The (Second Generation) Onion Router, which

is an onion routing protocol which does not use the Navy's patent and is freely available to anyone with an Internet connection.

TOR is the highest level of encryption, it's almost certain that neither the FBI nor anybody else can break it. TOR allows you to surf the Internet with (almost) total privacy. It does this by using a network of thousands (or more — total number unknown) of routing sites. When you connect to the TOR network, the data to and from your computer is encrypted automatically and goes to a TOR entry relay. From there it bounces to another TOR site, then to another, then another for some large random number of bounces, potentially all the way around the globe, encrypted the entire time. Then the data leaves TOR and accesses the normal Internet. However, the normal data bits that allow you to be identified as the user have been scrambled. TOR gives you a false IP address and periodically changes it.

From 2004, when TOR was first developed, until 2005, TOR was supported by the Electronic Freedom Foundation. Currently TOR is controlled by the TOR Project, a non-profit organization in the USA, which receives support from the U.S. State Department and the National Science Foundation. These people support TOR because they recognize that there are many good reasons why people need privacy on the Internet. In 2011, the Free Software Foundation gave TOR their Award for Projects of Social Benefit, stating "...Tor has enabled roughly 36 million people around the world to experience freedom of access and expression on the Internet while keeping them in control of their privacy and anonymity. Its network has proved pivotal in dissident movements in both Iran and more recently Egypt."[3]

China, which doesn't approve of Internet privacy, attempts to block all TOR traffic. It is believed that China inspects all Internet packets for TOR handshaking protocols and blocks all packets containing these protocols. There has been some success in recent months in sneaking TOR through the Great Firewall of China (using a technique called Obfsproxy relays), but the current status of TOR in China is uncertain.[4]

TOR is actually very simple to use. Go to www.torproject.org and download TOR for your computer. It's available for Windows, Mac, Linux and Android. It's free. Once you install it, you start a program called Vidalia, which connects you to the TOR network and opens a special browser that TOR installed (it is a specialized version of Firefox) which is configured to work with TOR. Your connection to the TOR network is encrypted — it apparently could be determined (see China above) that you are on TOR, but no one can tell what you're doing there. As long as you're using the TOR browser, your privacy is protected. If you want to send a truly private email, get yourself a Web-based email account that is not identified as belonging to you, and use it via TOR to send emails to whomever you want. If the recipient is using TOR to read his or her emails, then nobody can monitor your communication. If you are truly paranoid, you can PGP or AES encrypt the emails as well.

I call TOR "scary-level" encryption. It is true military-grade encryption — it was originally developed by the U.S. Navy. It's more than just encryption, it's an Internet hidden inside the Internet, the so-called "Darknet." TOR calls these the "hidden services." TOR allows the use of the .onion pseudo top-level domain. Websites can get a pseudo domain name through TOR that (since it is not a real domain name) can only be accessed through TOR. When you access one of these pseudo domain or hidden services via TOR, your data never leaves the TOR network and is always encrypted — the whole way from your computer to the hidden service website and back. As long as the encryption works, no one can tell that you visited a hidden website or what you did there.

Why am I almost certain the FBI cannot break TOR at this time? Well, besides the dissident movements in Iran and Egypt, guess who uses TOR? TOR is very popular with one particular class of people: criminals. If you get on TOR and look at the hidden services, many of them appear to be illegal. There are sites that will sell you stolen credit card numbers or hacked PayPal accounts. There are sites that will sell you illegal drugs. There are kiddie porn sites. There are sites where you can hire a hit man. If the FBI could identify who is running these sites, I suspect they would be shut down. Back in 2011, the hacking network Anonymous reportedly attempted to shutdown the kiddie porn sites on TOR. They managed to get and publish the IP addresses of 190 users, but the kiddie porn network is still very much up and running.[5] And Anonymous did not break TOR's encryption. Their hack involved tricking 190 kiddie porn users into

uploading a patch to their individual TOR programs that let Anonymous track them.

There are probably lots of ways to access these hidden services. The only way I'm familiar with is to get on TOR and access the "hidden wiki." Just do a search for hidden wiki or you can go to http://kpvz7ki2v5agwt35.onion.to/wiki/index.php/Main_Page. The content of this page changes from time to time, but if you look on the right hand column, there are links that will take you to all kinds of scary places. Just accessing some of these sites is possibly illegal, so I do not recommend that you do so. But I think it is good to be aware of how to access these sites, since some of your clients might be going there!

As a little extra, let me tell you one very simple technique you can use that might tell you if someone is reading your email. This happened to me several years ago. I had a friend working for an American engineering company that was building a power plant in Egypt. He was on-site in Egypt and we regularly corresponded by email. However, on several occasions, emails that I sent him did not appear to arrive and emails that he said he sent me never showed up in my inbox. I became curious. I ran a number of trace routes to his email server, similar to the ones I described at the beginning of this article. The path varied a lot, except it always went through an "extra" server right before it got to his mail server. I had no idea why that server was there. I asked my friend about it and he said that all the company's Internet was routed through a government server that provided them with Internet access. We both were wondering if our emails were being read and occasionally censored. So I set a trap: I uploaded a garbage file to an Internet dropoff/pickup service — I don't remember which one I used then but www.sendspace.com is available for this purpose now. Then I sent an email to my friend, telling him I had uploaded the file for him to download and described it in terms that would catch a would-be censor's attention. A couple days later, I confirmed that my friend had never received the email about my upload. Then I went to whatever dropoff/pickup service I used and they told me the file had been downloaded one time since I uploaded it. Since my email was the only way someone would know how to get to that file, we were pretty certain that someone really was reading (and censoring) our emails. So we started using PGP to encrypt all our emails. This got an immediate reaction. The people running the censor office complained to the local head of the engineering company that one of their employees was encrypting his email. The head of the engineering company got angry — not at my friend, but at the censor. You see, he had been doing his banking and investing by email, as well as communicating with his wife and family back in the states, and wasn't really happy about the idea that someone was reading his emails. He, and everyone else in the company, had been unaware that this had been going on. My friend told me that in a couple of weeks, almost everyone in the company was using PGP when they wrote home!

CONCLUSION

Internet privacy is important. Lawyers should be aware of how little privacy there is on the Internet if you are not using encryption. At the very least, some type of encryption should be used when sending confidential information over the Internet. The downside of really good encryption is that it allows people to do things on the Internet that are illegal. However, an argument can be made that this is necessary, as it also allows people to do things on the Internet that some governments consider to be illegal but that other people consider to be free speech.

1. www.schneier.com/blog/archives/2012/03/can_the_nsa_bre.html.
2. www.wired.com/politics/law/news/2001/08/46329 – or just Google "Nicodemo Scarfo pgp."
3. www.fsf.org/news/2010-free-software-awards-announced.
4. www.technologyreview.com/view/427413/how-china-blocks-the-tor-anonymitynetwork.
5. gawker.com/5855604/elaborate-anonymous-sting-snags-190-kiddie-pornfans.

ABOUT THE AUTHOR

Duane Croft practices family law in Norman. He earned a B.S. degree in physics/math from the University of Pittsburgh in 1979. He spent the next 20 years performing safety analysis engineering and accident analysis/investigation at several nuclear power plants. He graduated from OU College of Law, passing the U.S. Patent Bar in 2004 and the Oklahoma Bar in 2005.