Attorney Encryption Now!

CONSTITUTIONAL COMMUNICATIONS
CONCOMMS.ORG INFO@CONCOMMS.ORG

" We need new professional training and new professional standards to make sure that we have mechanisms to ensure that the average member of our society can have a reasonable measure of faith in the skills of all the members of these professions."
– Edward Snowden

Are your Attorney's data practices violating your attorney-client privilege?

How can you be sure your Attorney is upholding your human right to privacy?

Is your Attorney putting your privileged communication at risk?

Could evidence shared in confidence with your attorney be used in a case against you?

Attorneys are facing a crisis of data insecurity. 67 percent of IT Professionals reported that their organization experienced the loss or theft of data over the past two years.

Sometimes that theft of data was because of government interference with attorney client privilege.

(cont. next page)

What you can do:

1) Download the free Open Whisper Systems **"Signal"** or **"RedPhone"** open source encrypted voice and text app from your cell phone app store and have your attorney download it as well.

2) Sign the petition to the NY State Bar asking them to increase the attorney-client ethics to require default end- to-end open source encryption for client communications.

3) Support consumer protection bills that require that private entities encrypt the personal data of clients and consumers.

4) Become a member of Constitutional Communications, and help educate others.

5) Demand that your Attorney respect your right to privacy and uphold attorney-client privilege; make sure he or she offers default open source encryption for all client communication.

Government Attacks on Attorney-Client Privilege (cont.)

The US Government has taken privileged information from many US attorneys. They have taken information from Mayer Brown, a major Chicago-based law firm involved in trade negotiations, as well as from attorneys working on civil rights issues. Prosecutors have begun investigations on clients based on this illegal electronic dragnet information. Working though a $125 million unit of the Drug Enforcement Administration (DEA) multiple federal agencies access NSA databases and use a procedure called 'Parallel Construction" to hide evidence obtained through illegal mass surveillance of email and internet monitoring. The government then brings such evidence into cases where it would otherwise violate the 6th Amendment or be illegally obtained.

Unless your Attorney is properly securing your data, such evidence against you could have come from your Attorney.

To properly secure your attorney-client information, your attorney must use end-to-end open source encryption.

Frequently Asked Questions (FAQ):

1) Is email encrypted?

No, Email is a postcard when it travels across the internet. Encryption puts your postcard in a envelop.

2) How do I know if my Attorney is encrypting my communications?

Ask him or her to explain how your data will be handled in transit and at rest. Attorneys may be violating your attorney-client privilege, your privacy rights, or Massachusetts law if they don't have a PGP key that you can email on their website, or if they can't explain how your data is encrypted and secured at rest and in transit.

3) Isn't it too expensive for normal people to use encryption?

No, open source encryption costs nothing and more secure then proprietary encryption.

4) I don't have any thing to hide. Why do I need encryption?

If you are speaking to an attorney it is his or her responsibility to encrypt the communications for you. It is a lawyer's job to know if a prosecutor could consider that something you are innocently doing or saying could be a crime. But even when you are just writing friends, your communications should be private. As Supreme Court Justice Breyer elaborates: "The complexity of modern federal criminal law…make it difficult for anyone to know, in advance, just when a particular set of statements might later appear (to a prosecutor) to be relevant to some investigation."

For instance, did you know that it is a federal crime to be in possession of a lobster under a certain size? It doesn't matter if you bought it at a grocery store, if someone else gave it to you, if it's dead or alive, if you found it after it died of natural causes, or even if you killed it while acting in self defense. You can go to jail because of a lobster.

You have a free speech right, even when you have nothing to say, and you have a privacy right even when you have nothing to hide.

5) What is Open Source?

Open source software, such as Linux or Debian, allows for software engineers and users to fully control all aspects of a computer system. Proprietary programs, such as Microsoft and Apple Operating Systems, provide legal and technical prohibitions on users and engineers that keep them from viewing the actual functioning of the codes that make the computer programs run.

FAQ (cont.)

6) What is attorney-client privilege?

Attorneys have an ethical responsibility to protect client information. Rule 1.6 of the Model Rules of Professional Responsibility states that, “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client”. Attorneys who refuse to use encryption are leaving themselves open to hackers, the NSA, and adverse legal actions and significant fees against them.

7) What is encryption?

Encryption is simply - writing in code. Current encryption programs apply very rigorous math, logic, and technology to the basic process that all people engage in when creating dialects or languages. Current application of this science allows anyone with a home computer to create encryption advanced enough that it, when properly implemented, cannot be broken by all the computer power in the world. As Snowden has stated "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."

8) Can using encryption get you in trouble?

Encryption is legal in the US. When you use the Internet or a cell phone you almost always use some version of encryption. Encryption basics let your cell phone connect to the tower, are in the auto update function of your browser window, and are used every time you’ve paid for anything online. State law for private businesses in Massachusetts and Nevada require encryption use. A global survey of nearly five thousand businesses found that 35 percent of organizations now have an encryption strategy applied consistently across the entire enterprise.
In the United States, encrypted traffic has jumped from 2.29 percent of all peak hour traffic before 2013 to 3.8 percent in 2014, and in Latin America it has gone from 1.8 percent to 10.37 percent. However, the vast majority of communications today are not encrypted.

9) Why open source encryption?

Proprietary encryption has often been modified or “backdoored” to allow spy agencies, hackers, or criminals to get access to information advertised as “secure”. Skype, Blackberry, Snapchat, and RSA are only a few of the many companies that have advertised proprietary encryption products that we later found out were maliciously broken to allow spy agencies and hackers access to private communications. On the other hand, in over twenty years of use, open source encryption algorithms, like PGP and OTR, have maintained their security, even against agencies as well funded as the NSA.

10) But isn’t encryption expensive? Won’t it put small firms at a disadvantage?

Current open source encryption programs allow for free access to User side end-to-end encryption. Apps, like Signal or RedPhone, which has more than 500,000 users allow for free open source messaging. For more robust office privacy needs, PGP, Tails, and Tor are free open source programs used by thousands that offer secure document creation, sharing and web research.

FAQ (cont.):

11) But isn't encryption too hard for everyday use?

Encryption is a mathematical process that scrambles data to everyone except the intended recipient. You already use encryption everyday. You use an encryption enabled device when you close a garage door with a remote, buy a coffee with a credit card, swipe a smart card to board a train, use a cell phone to connect to a tower, use a wireless Bluetooth ear piece, or use an entry card system to access many buildings. These are just six uses of encryption before 9 am, there are dozens more by 5 pm.

12) What is Constitutional Communications?

Constitutional Communications provides digital security and privacy to civil society. We deliver the technology and competency required to maintain the privacy of data from mass surveillance and targeted attacks. We educate professionals about the legal standards necessary to uphold their client's rights and provide the communications tools to protect those rights in practice. We challenge professionals and governments to uphold consumer and client rights to the highest ethical standards.

13) Who is Constitutional Communications?

We are an organization of attorneys, technologists, entrepreneurs, consumers and clients, who fight for human and privacy rights and professional ethics in the information age. We are tired of professionals and government ignoring the security of our information. We take direct action to encrypt our data and pressure governments and professional associations to use open source encryption for all communication.