Privacy in the Modern Age, Part 5
Edward D. Duvall
3 May 2021

5 Personal Computers

It sure is convenient in these modern times to have the internet available; there is so much more information than there was back in the days of the Encyclopedia at the local library. But, take the bad with the good: there is also a lot of false and misleading garbage out there, too. At least the cigar-chomping old guys who wrote the Encyclopedia had their work reviewed by competent experts, and if it was in the Encyclopedia, you can be sure that the authors and reviewers believed that their articles were true and correct at the time it was written. The internet, on the other hand, is full of people who lie for a living.

There are a great many other issues to contend with regarding computers, the internet, and privacy. If you use a Microsoft or Apple operating system, you cannot actually delete a file. When you tell those operating systems to delete a file, all it does is delete the pointer to the first byte in the file, not the data itself. That means that all your files are still there, and anyone who understands how the file system and pointer system can recover anything that you thought you had deleted, including all your financial and personal data. The only remedy is to install special commercial software programs (Sdelete, ccleaner, or Eraser) that overwrite all disk space not actively being used (including the "deleted" files). However, if you use a UNIX-based operating system, it will in fact entirely delete a file, and overwriting is not necessary.

There are other risks that can compromise your privacy entirely. First, you do have control over what you download from the internet. But you do not have any way to control, or even to know, what is being uploaded from your computer whether you are on the internet or not. You, the PC user, are not provided with any tools that will allow you to see what is being sent from your PC without your express consent.

Second, we are all aware of the numerous "viruses" on the internet designed to shut your system down or encrypt your data until you pay a ransom to have it unlocked.

Third, the large tech companies are trying to convince you to store all your data on the "cloud", which is (of course) advertised "for your convenience". They even tell you that all your data is encrypted.

Fourth, most internet search engines (especially google and bing) track all your internet searches and maintain a list of all the websites you have visited.

Here are some suggestions to mitigate these direct risks. This is not foolproof, and it is only a first-order method; there are far stronger methods.
1. Never store anything on the "cloud". It may well be that your data is encrypted, but so what? What matters is who has the encryption key; and of course, no one is going to tell you what corporations or what government agencies have the keys. You should not assume anything you place on the cloud is actually kept private. Instead, use a separate external hard drive (a drive holding one terabyte now costs about $50), connected to your PC through one of the USB ports.

2. Never store anything of value on your PC's main hard drive. Store everything of any importance on the external drive only. Never store any financial records, personal data, pictures of yourself or your family, your driver's license copy, or anything of relevance on the PC hard drive, only on the external drive. The exception is that you can store individual documents on your PC hard drive only if they are encrypted. In

http://edduvall.com
edward.d.duvall@gmail.com

Edward D. Duvall is the author of The Federalist Companion: A Guide to Understanding *The Federalist Papers* and *Can You Afford That Student Loan*.

addition, use thumb drives as backups to the external drive (since the external drive will fail at some point).

3. Disconnect the external hard drive from your PC whenever you get on the internet. That way, if anything is being uploaded, only the things of no value can be uploaded without your knowledge.

4. Use strong passwords of important documents; this utility is found on nearly all commercial software products (although you may have to access the non-helpful "help" to gain access to how it works. Your password should consist of at least 10 characters, and be a combination of letters, numbers, and symbols. Do not store the password anywhere on the PC; instead, write them down in a small notebook and put them in a secure place elsewhere in your home or office.

5. Only use internet search engines that do not preserve a search history (such as DuckDuckGo, IXQuick, or StartPage). Do not use google or bing or any other ones that retain a search history.

http://edduvall.com
edward.d.duvall@gmail.com

Edward D. Duvall is the author of The Federalist Companion: A Guide to Understanding *The Federalist Papers* and *Can You Afford That Student Loan*.