All about Protecting your Data

Introduction

The world is awash in data, whether from the digital "bread-crumbs" we leave as we send another email, hit a friend back with a text, browse the internet, show our "likes" on Facebook posts, post comments on Twitter, and light up GPS data with our smart phones as we travel about our day, or the thousands of credit and debit card swipes we make every year. Additionally, the IoT (Internet of Things) continues to grow, with sensors, cameras, and other data-gathering devices (in addition to our smartphones, which are the ultimate data-gathering devices) increasing in number at an almost immeasurable rate.

Our data is all over. It's on our laptops, desktop PCs, smartphones, iPads, in the Cloud at such places as Carbonite, Microsoft OneDrive and online at Gmail, Yahoo Mail and many other places. So, how do we keep it secure. Not only do we need to secure our data now, but how about after we're gone. Do we need to think about our heirs?

This document will attempt to cover some of these issues, but only your legal advisor can give you the advice that's right for you.

There's a summary at the end for your convenience.

Protecting your PCs

What needs to be protected?

This is entirely up to you. The usual suspects include documents, photos, music, passwords and videos. You shouldn't keep any sensitive data on your PC including passwords, Social Security Numbers, health data etc. The ultimate PC security is if your PC is stolen and nobody can access your data, even if they remove the hard drive and connect it to their own PC.

Levels of Protection

- Start off by backing up all your data to an external hard drive and keep it in a safe place. You may also decide to encrypt the drive using BitLocker or the free VeraCrypt.
- Encrypting your data
    - Level one – use a Microsoft Local Account with a password. Anyone can crack this easily. Not recommended.

- Level two – use a Microsoft Administrator Account. This is secure if you sign out after each use. Be sure to use a strong password and don't leave it lying around.
- Level three – use Device Encryption which is available on a handful of PCs including the Microsoft Surface Pro. You can see if you have this feature by going to Windows Settings, System, About. If you don't see Device Encryption listed, it's not available.
- Level four – BitLocker. This is only available with Windows 10 Pro and must be enabled to be effective. Read more here. If you have Windows 10 Home edition, it will cost you $100 to upgrade to the Pro version. With BitLocker, it's virtually impossible for someone to access your data if they should steal your PC provided you have logged out of your PC. Note – you can also use BitLocker on a flash drive or external hard drive if you wish to store sensitive data on it. This feature is called BitLocker To Go.
- Example – on a PC with BitLocker, I plugged in an external hard drive and opened This PC. Next, I right-clicked it and selected Turn on BitLocker. I followed the directions and entered a password. Next, I ejected the drive and plugged it in on a PC without BitLocker. I right-clicked the drive and selected Unlock Drive and entered my password. The moral of the story is that you can encrypt any flash drive or external hard drive with BitLocker and unlock it in any other PC if you know the password. This is a great way to store personal data.
- You can also use a free program called VeraCrypt as seen here, there is excellent help at their web site. This is an alternative to BitLocker.

Protecting individual documents

- There are several ways to do this including encryption and password protection.
  - For encryption you can use VeraCrypt as discussed above
  - For password protection, see the article here.

Avoid statements by mail

Believe it or not, getting statements electronically is more secure then the US Mail. This way, no one can steal mailed statements from you.

Protecting your online data

Types of online data

- Services that you use such as email and cloud storage
- Social media accounts such as Facebook
- Online accounts such as banking, Medicare, Secondary Insurance, Microsoft Account and so on.
- Shopping sites including Amazon, Target and the others that you have shopped with. Many of these ask to store your credit information for faster access in the future. Not to easy to keep track.
- Note – one way out of this mess is to change credit cards.

Securing your online data

- One of the best ways to protect your online data is to use Two-factor Authentication. Many banks offer this service as does Microsoft, Amazon, Yahoo and others. You must register with a mobile phone as an alternate way to contact you. In this way, no one can log into your account without your phone. You can read the instructions for most services on line by searching. The instructions for Amazon, for example, are here.
- Another way to stay safe is to not write all your passwords on a piece of paper or in a notebook which can be easily lost or stolen. Use a password manager instead. This way, you only must remember one password. Several password managers include LastPass and RoboForm. They're not free but they're secure.

Protecting your mobile devices

Using Fingerprint or Face Recognition

Remote Wiping

- Be sure you have Find My iPhone enabled. Go to Settings, your name, iCloud. Scroll down to Find My iPhone and make sure it's enabled. See the instructions here to wipe your iPhone.

Avoid Open Wi-Fi networks for banking and other financial transactions

- This is safe for web surfing but unsafe for most other tasks.

Record your IMEI

- Go to Settings, General, About to see the IMEI.

Backup device regularly

- Go to Settings, your name, iCloud and turn on iCloud Backup

How to prepare for your digital afterlife

Make sure your accounts end up in the right hands when you die. You're probably not going to die any time soon (knock on wood), but it's never a bad idea to prepare for the worst. Your will may take care of who gets your car when you pass away, but what about who gets your Facebook account? Or who's allowed to access your Gmail data? Managing your digital after-life can be tough, especially if you have a lot of data hidden away within the depths of your inbox. Here's what you need to know about how you can leave your accounts in good hands when you die --and what companies will (and will not) reveal to your digital heirs.

Google

Google doesn't explicitly talk death, but they do let you decide what happens to your Google accounts --Gmail, Photos, Google Drive, etc. --when you haven't signed into your Google account for a period. Google lets you add up to 10 friends and family members who will be notified if your account is in-active for a certain amount of time, and who will (with your permission) be able to download data from your accounts for three months.

Microsoft

If you have a Microsoft email account (Hotmail, Live, MSN, or Outlook.com), family members will need to go through Microsoft's Next of Kin process in order to gain access to your account data. Microsoft will release your account data -- including emails, attachments, and your address book --to your next of kin on a DVD. Your next of kin will not receive your password or be able to access your ac-count (just the data).To start the Next of Kin process, your next of kin will need to email msrecord@microsoft.com and provide documentation that verifies that you are dead (or otherwise incapacitated) and that they are your next of kin, the executor or benefactor of your estate, or someone with power of attorney.

Yahoo

Yahoo will not release any of your data when you die, so if you want your family to be able to access your account you will need to provide them with your login information (though Yahoo's Terms of Service states that your account is not transferable, so technically providing your login info to your family is breaking their rules).While Yahoo will not share any of your data or ac-count information, the executor of your estate/next of kin can request that your account be closed

through this request process from Yahoo, which will require a request letter containing your Yahoo ID, as well as proof of your death and proof that they are the executor of your estate.

Facebook

Facebook allows you to designate a legacy contact who can manage parts of your account when you die. Legacy contacts cannot sign into your account or see any private messages, but they can post a pinned post to the top of your Timeline, accept (or reject) new friend requests, and update your profile picture and your header image. They can also (with your permission) download an archive of your posts, photos, and profile information. Learn how to assign a legacy contact here.

Twitter

Twitter does not allow you to grant anyone access to your account when you die, though immediate family members and people who are authorized to act on your behalf can request that your account be deactivated when you pass away. If you want someone to be able to take over your account when you die, you'll need to provide them with your login information. To request that someone's account be deactivated, you will need to use Twitter's privacy form. You will need to provide proof of your relationship to the deceased, including your ID and a copy of their death certificate.

Instagram

Instagram is owned by Facebook, but the photo-based social network does not offer the same post-mortem option of designating a legacy contact. How-ever, Instagram does memorialize accounts --memorialized accounts cannot be changed or logged into, but they will remain visible and will not appear in Instagram's public archives (like Search & Explore). Your friends and family members will need to con-tact Instagram about memorializing your account after you die, according to Instagram's Privacy Policy, using this form. They will need to provide their name and email address, the deceased's name and Insta-gram username, and proof of death, such as a link to an obituary or a death certificate.

Password Managers

Even the accounts that do let you designate a digital heir don't let people fully access your stuff after you die. If you want to leave full access to your accounts

to someone after you pass away, your best bet is to use a password manager with a legacy feature. LastPass has an Emergency Access feature that lets you give trusted contacts access to your password vault. To add a trusted contact, open your LastPass account and click Emergency Access. Click Give Emergency Access and type in your contact's email address. Choose a wait time for how long that contact will have to wait when they request emergency access (anywhere from "immediately" to 30 days). If your contact requests emergency access, you will have this amount of time to reject their request before they are automatically granted access.

Dashlane also has an emergency access feature that lets trusted contacts request access to your vault, while PasswordBox features a Legacy Vault that lets you pass on your passwords to your next of kin.

Dealing with Google Activity

- Google saves much if not all your search data. You can manage this or delete all activity by going to www.myactivity.google.com.
- Click **Delete activity by** to see the options
- Click **Activity controls** to enable Web and App Activity
- Go to www.myaccount.google.com/activitycontrols to control what Google tracks.

Passing on your Frequent Flyer Miles

- The site here and here may help with this.

Cancelling someone's online accounts

If you're worried about an online account such as Facebook and want to cancel the account, one of the sites below will help you.

- Account Killer click here.
- Everplans click here.
- Just Delete Me click here.

Resources

- Using BitLocker click here.
- Device Encryption click here.

- VeraCrypt click here.
- Beginner's Guide to encryption click here.
- Amazon Two-Step Verification click here.
- iCloud Two-factor authentication click here.
- Microsoft Two-step verification click here.

Summary

Here a list of things you can do. All are described above.

- Password protect individual files
- Encryption entire PC with BitLocker
- Encrypt external hard drive or flash drive
- Use two-factor authentication
- Delete online accounts
- Use passcode or facial recognition on mobile devices
- Enable Find My iPhone
- Backup your iPhone