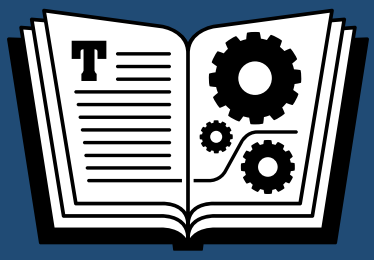
EBOOK EXTRAS: v1.0
Downloads, Updates, Feedback



TAKE CONTROL OF

YOUR DIGITAL LEGACY

by JOE KISSELL

$15

Table of Contents

Read Me First

Welcome to *Take Control of Your Digital Legacy,* version 1.0, published in January 2017 by TidBITS Publishing Inc. This book was written by Joe Kissell and edited by Tonya Engst.

This book walks you through the process of digital estate planning. It helps you identify the important information you may want to pass on to future generations, document your wishes in detail, and make practical decisions about preserving your data.

Discounted classroom and Mac user group copies are available.

Updates and More

You can access extras related to this ebook on the Web (use the link in Ebook Extras, near the end; it's available only to purchasers). On the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy any subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading on mobile devices on our Device Advice page.)
- Read the ebook's blog. You may find new tips or information, as well as a link to an author interview.

If you bought this ebook from the Take Control Web site, it has been added to your account, where you can download it in other formats and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually; see Ebook Extras.

Introduction

I turned 50 on January 9, 2017—a little over 21 years after I started writing books about technology. For whatever reason, much of my audience over these years has been a generation or so older than me. I constantly get email from readers in their 80s and 90s, and when I speak to user groups, I'm often the youngest person in the room by a considerable margin.

For a long time, this phenomenon was a mere curiosity, and I didn't consciously tailor my writing to an older reader. But then I started noticing that lots of the questions and comments I received had to do with topics I hadn't thought very deeply about myself: namely, how to deal with files, photos, email, online accounts, and other digital items when their owner died or became unable to handle them personally. People would come up to me after a talk about passwords or backups and say something like, "Well, I'm 89 so I won't be around much longer, and I want to make sure my son can get into my accounts when I'm gone," or "I'm trying to figure out how my great-grandchildren will be able to read my documents 50 years from now."

Those questions deserve answers, and that's what I aim to provide in this book. Your digital legacy—whether, how, and in what ways your data will carry on without you—is a hugely important topic in the 21st century. No matter your age or health, something *could* happen to you at any time, and having a plan in place to deal with your accounts, files, and other digital data is a great kindness to your family and friends—to say nothing of future generations who may want to know all about you. (And, lest this all sound terribly morbid, the very same steps can be equally useful to someone who needs to take care of business for you temporarily if you're sick, injured, or even just on vacation.)

We have tools such as wills and trusts to spell out what should happen to our physical and financial assets, but more often than not, those instruments say nothing about our incredibly valuable digital assets. Maybe you have tens of thousands of beautiful family photos, but what if they're on an encrypted computer and no one else knows the password? What will become of your Web site, Facebook account, or email if you alone know how to access it, and leave no instructions? And what will happen to all the data you've trusted to various cloud services when your credit card expires and no one else is paying the bills?

These are just a few of the many questions I help you answer in this book. I walk you through the process of inventorying your digital assets, figuring out what to do with each of them, drafting a digital will, choosing a digital executor, and much more. I also talk about information that isn't currently digital, but maybe should be if you want to preserve it for a long time—things like paper photos, analog video and audio tapes, and important family documents. And I discuss at length the nuts and bolts of decisions you'll have to consider like which file formats and physical media you should use to preserve data for posterity, whether you should entrust any of this data to a cloud service, and how to be sure all your preferences are clearly spelled out.

In short, this book is about digital estate planning. It's not going to teach you new tech skills or get you excited about the latest apps and gadgets, but I've done my best to make this essential topic interesting and engaging. By the time you've finished the steps in this book, you should be confident that your data will be in good hands when you're no longer able to manage it. In the process, you may just find yourself becoming more organized and better prepared for random, fleeting emergencies too.

In much the same way that a book could walk you through the mechanics of writing a will but not tell you which assets to leave to

whom, I can't give you precise step-by-step instructions for everything, because each person's situation is unique. My goal, instead, is to provide a thorough framework that will help you identify what you need to do and make smart decisions about how to carry out your plans.

Whether you're 25 or 95, and regardless of which devices or operating systems you use, I hope you'll find the resources here to put your digital affairs in order—and, with any luck, have some fun doing so.

What If I Can't Do Everything in This Book?

Please don't feel you have to follow every suggestion in this book, in detail. Of course, you're entirely welcome to do so, but depending on the amount and types of digital data you have, it could take quite a while to get through everything. As you develop your own digital estate plan, you can incorporate as little or as much of this information as makes sense to you, and in any order.

Even if you accomplish only a fraction of what this book describes, you're still taking important steps toward preserving your digital legacy and helping your family and friends make the most of your data.

Quick Start

In this book I lead you through a process of compiling, documenting, and preserving information that you'll leave for future generations. For the most part, later topics build upon earlier topics, so I strongly recommend reading the book in linear order. (You may, however, choose to skip chapters or topics that don't apply to you.)

Take preliminary steps:

- Learn about the benefits and challenges of planning for your digital legacy; see Envision Your Digital Legacy.
- Make detailed lists of your major types of digital data in Inventory Your Digital Assets.
- Decide what types of data you'll preserve for the future, who will handle your digital estate, what file formats to use, and more; see Make High-level Decisions.

Prepare major categories of data for archiving:

- Scan (or have someone else scan) and organize photographs and documents that currently exist only on paper; see Digitize Photos and Documents.
- Make sure someone else will have the usernames, passwords, and other details necessary to access all your accounts; see Deal with Passwords.
- Provide instructions for both ongoing access to your email account(s) and how to deal with all your saved messages; see Deal with Email.
- Decide whether your social media accounts should be preserved (online or offline) and whether any final messages should be posted; see Deal with Social Media.

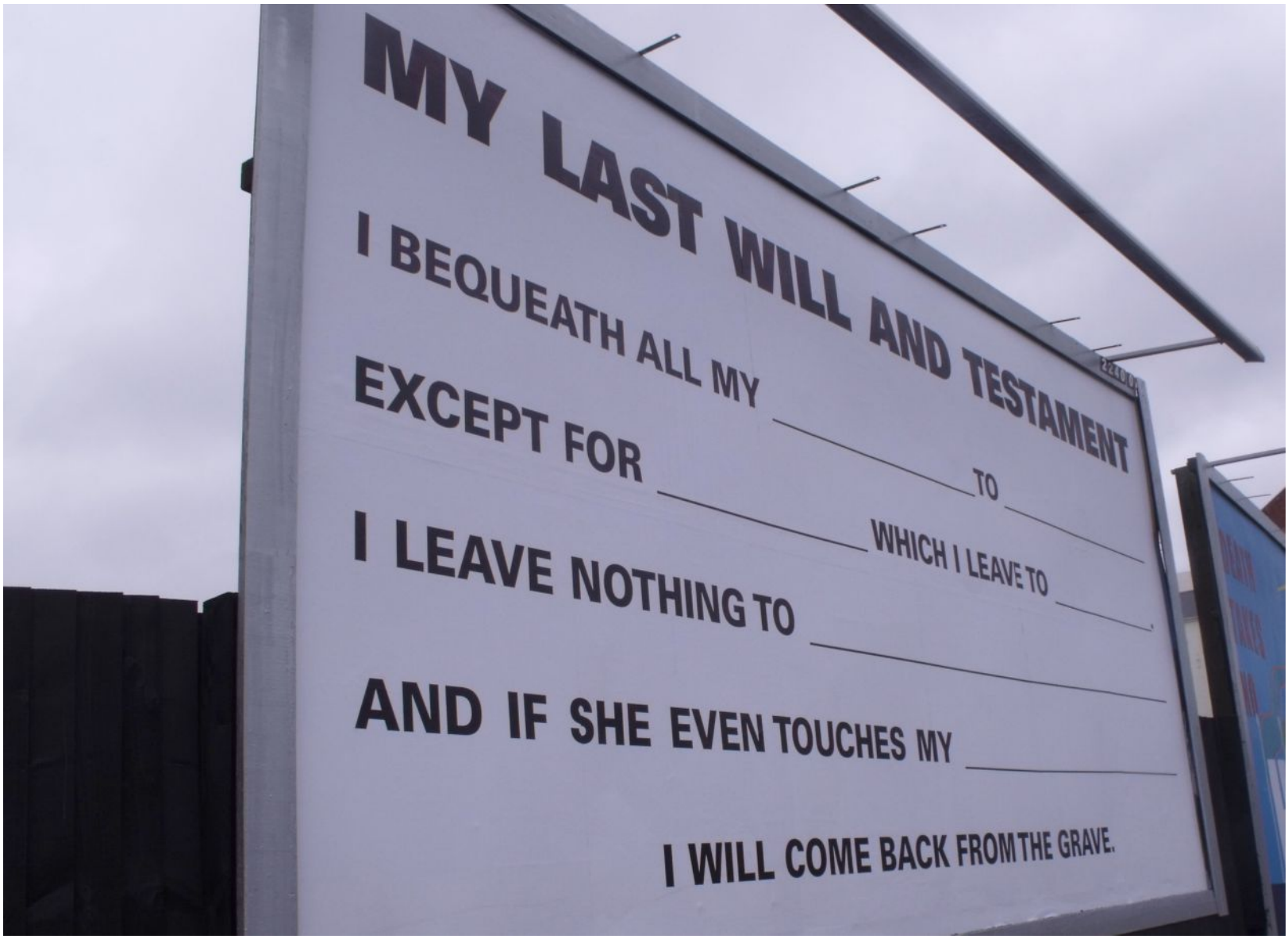
- Make decisions about the files and software on your computer and in the cloud, plus backups and other miscellaneous items; see Deal with Other Digital Data.

Assemble the pieces:

- Make one or more copies of your digital data on media that's likely to last quite a while; see Preserve Your Data for Posterity.
- Create a file that includes your digital will, your data, detailed instructions, and other components of your digital legacy; see Create a Legacy Dossier.

> **Note:** As you work through this book, you'll be creating a digital will, as I discuss in Begin Drafting Your Digital Will. At any time while reading this book, you can download a Digital Will Template, in RTF format.

Envision Your Digital Legacy



Your digital legacy goes beyond the possessions in your will to include a lifetime of data.

I know almost nothing about my paternal grandfather, who died a few months before I was born. I've seen photographs of him, examined census records in which his name appears, and heard a few stories, but that's about it. And of his parents I know even less. There are complicated reasons why so little information about these family members

survived, but the fact remains that whatever documents or genealogical data I might dig up, I'll never be able to know what they were *like*. What were their interests, hopes, beliefs, and fears? Did they have a sense of humor? How did they interact with other people? Were they kind or cruel, interesting or dull? The answers to all such questions are beyond my reach.

By contrast, my descendants should have a bountiful supply of information about me. During my lifetime I've written many thousands of pages of books and articles, recorded hundreds of hours of audio and video, bared my soul in innumerable email messages, and posed for countless photos. I don't fancy myself a person of particular historical significance, but I would at the very least like family members in future generations to be able to find out what sort of person I was—what made me tick. And as long as I preserve all that data carefully, they'll be able to do just that. They won't have to rely on faded photos in a shoebox and half-forgotten, second-hand stories. And whether they consider me a hero, a villain, a champion, or a loser, at least their feelings about me will have a pretty strong basis in reality.

That's a big part of how I envision my own digital legacy. In this chapter, I want to help you get a sense of what yours might entail. Crucially, that includes not just the things you'll preserve for future generations, or even the stuff you'll want your next of kin to know about in the days leading up to your funeral. It also entails information and concrete steps that can improve your life today (see How Digital Legacy Planning Can Improve Your Life Now). At the same time, the complexities of preserving your digital legacy may be more involved than you imagine, and I hope to give you a realistic overview of the challenges you'll face (see Understand the Challenges). I also offer a few quick reminders about conventional, non-digital estate planning that you'll want to take action on if you haven't already done so (see Review: Estate Planning Basics).

What Your Digital Legacy Means

I've given some examples of what I mean by a digital legacy, and although the details of your vision may differ from mine, the underlying concept is this:

You get to make decisions now about what will happen to your digital data after you're dead—and far into the future.

If you're a public figure, or if you've done things that people are likely to write about in history books a century from now, you've probably already begun to take steps to insure that future generations look back on your life in a complimentary way. But even those of us who consider ourselves ordinary folk usually care about how we'll be remembered by our friends, family members, and descendants. My great-grandchildren, should I have any, probably won't see a statue of me in the park or sing songs commemorating my mighty deeds. But they might like to know what Grandpa Joe was like way back in the olden days of the early twenty-first century, because their lives will have been shaped, in part, by my choices.

Your actions, and the chains of events they cause, are part of your legacy. Your possessions, and indeed your family members themselves, are part of your legacy too. But in this day and age in which nearly everything is digital, when most people carry supercomputers (with built-in cameras, microphones, and video recorders) wherever they go, and when your every thought and emotion can be instantly transmitted around the world via social media, the data you create and accumulate over a lifetime is likely a larger part of your legacy than your money and house. It will almost certainly last much longer, too!

So, when I speak of your digital legacy, I'm thinking of the following:

- Digitizing aspects of your life (such as old photos) that are still analog

- Making crucial digital information about yourself accessible to the right people, in the right ways, at the right times (and, as a corollary, destroying information that you *don't* want to persist)
- Caring for your loved ones immediately after your death by providing them all the information they need to handle your affairs and your digital assets
- Enabling future generations to have as much information about you as you like

> **Note:** I say more about the immediate, short-term, and long-term aspects of your digital legacy a bit later, in Determine Your Priorities.

Whether your fondest desire is to be remembered forever or to be forgotten immediately, you can craft the digital legacy you prefer. But if you do nothing, your legacy will be entirely in the hands of other people, with lives and preferences of their own, and however much care they devote to preserving your data, it may not turn out the way you would have liked.

How Digital Legacy Planning Can Improve Your Life Now

Apart from giving you greater peace of mind, a regular will won't do much to improve your life right now. But planning for your digital legacy can serve lots of purposes while you're still alive. For example:

- **Better organization:** If your digital documents, photos, and other files are stored in a careless or haphazard way, you may decide that it's time to organize them in order to help anyone who may need to find things after you're gone. But guess what? Better organization will also make it easier for *you* to find things, reducing clutter and enabling you to work faster and waste less time searching.

- **Improved sharing:** Your friends and family members may enjoy seeing photos, old documents, and other artifacts that are currently stashed in a box, but that you'll scan as part of your digital legacy preparations. And (per the previous point) even items that are already digital, such as videos and music, are easier to share if they're well organized.

- **A backup plan:** When my wife and I go out for the evening, we write instructions for the babysitter. When I had a conventional job and took time off for a vacation, I'd leave instructions for my colleagues on how to handle my tasks in my absence. One of the things you'll be creating as part of your digital legacy is a similar—but more detailed—set of instructions that a friend, loved one, or other trusted person can follow to take care of any crucial business or personal tasks that, at this moment, only you know how to do (see How to Be Me).

  Those same instructions can enable someone to take over for you temporarily if you go on vacation, or become sick or injured. Plus, they can help you remember how to do tasks you perform infrequently, so you don't have to figure them out from scratch each time.

In addition, you may well undertake improvements in the ways you back up your data and handle passwords; eliminate unneeded accounts, files, and apps; learn more about your family history; and even get to know yourself a bit better.

Understand the Challenges

Leaving your house or your car to someone is relatively simple. I mean, it's not *truly* simple, as in merely handing over a key—there's all sorts of paperwork, and there are legal and tax considerations, and so on. But there are also well-worn procedures in place for facilitating such handovers, and if your will states that your son gets the house, then there's little else you, while still alive, need to do to make that happen; your son (along with your executor, lawyer, spouse, and other relatives) will deal with all the irritating details when the time comes.

At first blush, it may seem as though your digital data is far easier to pass on. If your data is on a computer, why, someone can just take your computer and have all your data, right? Well…kinda sorta maybe but not really. Preserving your digital data for the future is in fact considerably more challenging. Here are just a few of the reasons:

- **Encryption and passwords:** I'm a big proponent of using encryption and strong passwords, but the very tools that keep your data safe now can make life difficult for your heirs. If your computer's data is encrypted—for example, using FileVault on a Mac, or Device Encryption, BitLocker, or TrueCrypt on a PC—no one will even be able to boot the machine, let alone read your files, without your password. Similarly, the passwords for your online accounts protect them from snooping and identity theft, but someone else may need to access those accounts when you're gone. I talk about account access issues in Deal with Passwords.

> **Note:** There's a flip side to account access, which is that you may want to *prevent* anyone (or just particular people) from accessing certain files or other data–for example, by encrypting it and deliberately withholding the password. Either way, it's something you should consider and act on while you still can.

- **File formats:** I know a lot of people who, years ago, created tons of documents using software called AppleWorks. But that software was discontinued, and nowadays, even apps that convert AppleWorks documents to more modern formats are getting hard to find. The same is true for many file formats—what's easily readable today might be completely opaque a decade or two in the future. Even if you have a current app that opens your files readily, who knows if that app—or something comparable—will run on the devices and platforms that will exist years from now. I discuss these problem in Decide on File Formats.

- **Hardware and media degradation:** Nearly all kinds of digital media, from floppy disks and hard drives to CDs and DVD—and even flash drives—suffer random data loss over time. Whether the media itself physically degrades, a magnetic charge dissipates, or a cosmic ray flips a value from a zero to a one (or vice versa)—and yes, that really happens!—data can, over time, develop errors or even become completely unusable. Hard drives can also suffer mechanical failures that render them worthless, regardless of whether the data itself is intact.

  And who knows what interfaces will exist on tomorrow's devices? In the 1990s, computers and peripherals often had SCSI ports, for example, but I have no idea how I'd go about reading data from a SCSI drive today. I cover issues like these in Preserve Your Data for Posterity.

- **Organization:** Even if someone in the future can read all your data on some storage device, how will they find anything of value? My computer has well over a million files, including more than 200,000 email messages. Sure, someone can search all that data for a word or phrase, but no one will know, unless I spell it out, that an oddly named file deep in a forgotten folder hierarchy is actually a fragment of brilliant writing that was part of a novel I never finished.

In other words: you can't search for something if you don't know what you're looking for, and I don't think anyone is going to take the time to examine a million files individually just to see if I might have used a clever turn of phrase in one of them. I discuss organizational issues in Inventory Other Personal Data.

> **Note:** Yet another challenge involves Digital Rights Management, or DRM. I discuss this later in An Aside: Digital Media Complications.

For these and many other reasons, the task of ensuring that all (and only) the right people can access your crucial data in the future is more complicated than it initially appears—and that's exactly what this book aims to help you with. Every issue can be overcome with careful thought and planning.

Review: Estate Planning Basics

Your digital legacy is intended to be a part of your overall estate plan—not a substitute for it. If you haven't already dealt with the other steps, I urge you to do so—perhaps even before following the instructions in this book. Life is too uncertain to leave these important things to chance.

I am not by any means an expert in conventional estate planning, but as a quick reminder, a typical person will want to include (at least) the following elements:

- **A will:** This legal document spells out what will happen to your possessions when you die. It will name your *beneficiaries* (who will receive items you now own) and the *executor* (who will manage your estate and carry out the distribution of assets).
- **Guardianship:** If you have minor children, adults for whom you have legal responsibility, or pets, your will (or a separate document) should specify who will care for them after your death.

- **A living will (or advance directive):** A living will spells out what you want to happen (particularly in terms of medical treatment) if you are still alive but unable to make decisions for yourself.
- **Power of attorney:** A power of attorney gives another person the right to make certain legal decisions on your behalf while you're still alive. (Often, a living will and power of attorney go hand in hand.)
- **Trusts:** A trust is a legal agreement to transfer property to someone else (a trustee) who will hold it for the benefit of one or more other people (beneficiaries). Some trusts take effect while you're still alive, while others kick in only after you die. A lawyer can advise you as to the situations in which a trust is helpful.
- **Life insurance:** Whether just to pay for your funeral or to provide living expenses for your family after you die, life insurance is a wise investment for most people.

All these elements come in many varieties and are governed by rules that vary by jurisdiction. If you're just getting started with estate planning, a site like GYST can help you find the resources to work through each of these items. Some of them you can do yourself (possibly even for free), while others will require the paid services of a lawyer or other professional.

Inventory Your Digital Assets

Your computer is a virtual warehouse, with many thousands of files. Knowing what you have is a crucial first step.

When you're writing a will, it helps to have a fairly detailed list of your tangible assets—home, car, money, furniture, artwork, and so on. Perhaps you're leaving most of your estate to your spouse and kids, but you know your nephew has always loved that old cuckoo clock in the hall, or your neighbor would be thrilled to have your woodworking tools, and you want to make sure each item goes to the right recipient.

Many of your digital assets are qualitatively different in that they can (if you wish) be left to more than one person—for example, you can give everyone you know a copy of your entire digital photo album, effectively for free. However, you may not truly own some of your digital assets; items like software, music, and movies might simply be licensed, which affects whether or how they can be passed on. And other digital assets, like online accounts and digital currency, come with additional legal and logistical issues.

Rather than leave it to someone else to sort through this stuff later, I suggest starting now to create a list of your digital assets, including notes about how key data types are organized. Because your inventory of digital assets will form part of your digital will, I begin by helping you start that document. Your inventory will help you Make High-level Decisions about how to prepare your digital legacy, which will in turn inform the rest of the process.

Begin Drafting Your Digital Will

Unlike your regular will, which deals with your physical assets, money, and so on, your *digital will* is an informal document that contains instructions on the disposition of your digital assets.

A digital will doesn't have to be fancy, and it doesn't have to follow any specific format. It can be a simple document you create in your favorite word processor and then print out and keep with your regular will. Depending on the extent and nature of your digital assets, it might be just a few pages long or it might be much more extensive.

> **Tip:** To prevent confusion, you might want to attach your digital will to your regular will, and ideally, include a line in your regular will referencing the attachment–for example, "See attached Digital Will for further instructions on handling my digital assets."

In any case, I recommend starting this document now. Although you're free to create your own from scratch in any word processor or text editor, I'd like to offer you a shortcut: a downloadable Digital Will Template in RTF format, which you can edit as needed. At various points in this book I'll ask you to fill in details applicable to certain types of data. For the time being, add your name at the top (in the heading "Digital Will for *your name*"), and then include a sentence or two explaining the purpose of the document. For example, something along these lines:

In the event of my death, I would like my electronic files, digital photos, online accounts, and other digital assets to be managed as described in this document.

As you go through the remainder of this chapter, you'll type into this document the inventories of your various digital assets, which will includes a description of the way you've organized your files, email, and photos. Your inventory won't initially specify what should be done with those items, but you'll add those details later. By the time you're done working through this book, your digital will should contain fairly detailed instructions for dealing with all your digital assets.

Inventory Online Accounts

If you purchased this book online, you have an account with Take Control Books, Apple, Amazon, or another online ebook distributor. That account is likely just one of dozens if not hundreds of accounts you have for online stores, social media sites, email providers, storage and backup services, discussion forums, and other businesses. Some of your online accounts are much more important than others, but you should be able to list at least the most significant accounts—those that someone else will have to deal with in some fashion after your death.

If you already Use a Password Manager to store your usernames and passwords for all your accounts (good for you!), that can effectively serve as your inventory, although (as I discuss later), you should mark your most important accounts to make them easier to locate.

In fact, if you have more than a dozen or so accounts, this would be an ideal time to start using a password manager—you might want to set one up instead of making the handwritten list that I describe next—see Deal with Passwords, later.

If not, start a list in the inventory portion of your digital will right now. You might not be able to remember all your accounts offhand, but as you go about your normal routine and encounter sites and services for which you have an account, you can add them to your list. (Skimming through your saved email for messages confirming the creation of new accounts can also help.)

I suggest dividing your list into three main categories: Email, Social Media, and Other Accounts (all described ahead).

Email

List all your email accounts (that is, the provider name and your email address). If you have only one email account, this will be a short list! But many of us have multiple accounts. Be sure to include any accounts you have with providers such as:

- Apple iCloud (icloud.com, me.com, or mac.com)
- Gmail (with or without a custom domain)
- Microsoft (Hotmail, Outlook.com, etc.)
- Yahoo
- Your local ISP (Comcast, Cox, Time Warner, etc.)
- Other stand-alone email providers (like Fastmail.fm and Hushmail) and Web hosts (like GoDaddy and 1&1)

We'll return to this list and decide what to do with each account later, in Deal with Email.

Social Media

Add to your inventory a list of all your social media accounts. Just to jog your memory, here are some of the most popular services that fall into this category:

- Facebook
- Flickr (part of Yahoo)
- Google+
- Instagram
- LinkedIn
- Pinterest
- Tumblr
- Twitter
- YouTube (part of Google)

I explain your options for how these accounts can be handled after your death later, in Deal with Social Media.

Other Accounts

You may have hundreds of other accounts besides email and social media, but you don't need to list every single one. Instead, think of as many as you can in the following major categories:

- **Accounts you pay for:** Make a note of any account that requires a monthly or annual fee, such as Apple (Apple Music, iCloud storage, iTunes Match, etc.), Netflix, Spotify, Dropbox, Backblaze, Crash-Plan, your ISP, your domain name provider, and your Web host.

Because someone will need to either cancel these accounts or keep paying for them, they're especially important to know about.

- **Accounts with monetary value:** List accounts that contain money (banking, ecommerce, investments, PayPal, and so on—as well as affiliate programs and other sites that might owe you money), plus those that can be used to acquire goods and services (frequent flier programs, reward programs, and suchlike).
- **Accounts with valuable documents:** Think about, and make a list of, any accounts that enable you to access your medical and financial records, utility bills, and other documents that may not exist on your computer, and that someone may need to access after your death—to download the documents, cancel the accounts, or take over management of them.
- **Accounts used to communicate:** Besides email, you may have accounts for instant messaging, voice or video chats, or online telephone numbers—for example, Skype, Google Voice, AIM, Jabber, and Vonage.

We'll return to this list of accounts at a couple of later points in the book, when we Deal with Passwords and Handle Other Cloud Data.

Digital Business Assets

If you run a business that is small enough, or informal enough, to have no plan for dealing with your death, and if this business has an online component—say, one or more Web sites, cloud services, or even a personal blog that features ads or affiliate links—be sure to list all the details in your inventory. Your digital executor will need to know not only how to access the accounts themselves but also how your assets interrelate. For example, it's one thing to know how to edit posts on your blog, and another to know how to access your Google AdSense account, which displays ads on that blog and generates income.

In general, your conventional will should specify what will happen to any business assets after your death and who will take responsibility for managing the business's affairs and finances. However, your digital will should at least indicate which of your business assets have a digital component and how to access them.

Inventory Your Media

Media such as music, movies, TV shows, and ebooks is available in digital form from countless sources, and you may well have an extensive collection. Although you need not list every last song and TV episode, it's worth making a high-level list of what media you have.

For the purpose of your inventory, ignore streaming media accounts such as Netflix, Spotify, and Apple Music (although those should be noted in your inventory of online accounts), and include only media you've *downloaded* (or copied from another source, such as a CD or DVD) such that you can play or view it repeatedly without paying an additional fee or having to transfer the data again from the cloud.

For now, all you're doing is making a list. Well, two lists—one for media you've purchased and one for other media. You'll refer to these lists later when you make decisions about what to do with the items on them; see Handle Your Media. If you use iTunes, Plex, iBooks, or other such apps to organize your media, open them now; otherwise, you may need to look through folders on your disk or receipts to compile the lists.

List Purchased Media

Purchased media could have tax implications, just like your other tangible assets (talk to your lawyer or accountant for details); in many cases, it is also licensed rather than sold (see An Aside: Digital Media Complications), meaning that unlike other kinds of digital assets, you can pass it on to, at most, one heir. And, because this media is, by

definition, not unique (anyone can purchase it, so there are many copies floating around), it's of far less historical interest than data you created yourself. All these elements make it important to inventory this media separately from media that was not purchased.

Because I'm not in favor of busy work, and because it's not going to be useful to you or your heirs to have a track-by-track listing, I suggest that you put a few bullet points on your list with summaries of various media types. The main things to include are what sorts of media you've purchased and from which source.

Do this for music, movies, TV shows, and ebooks—something along these lines:

- **Music:** 539 tracks from iTunes. 28 albums from Amazon. 3 albums from Bandcamp. 138 albums ripped from CDs I own.
- **Movies:** 67 movies from iTunes. 99 movies ripped from DVDs I own.
- **TV shows:** 667 episodes from iTunes. 25 series ripped from DVDs I own.
- **Ebooks:** 72 ebooks from the iBooks Store, 45 from Amazon, and 29 (without DRM) from Take Control.

> **Tip:** To see how much media of a given type you've purchased in iTunes, first choose a media kind (such as Movies) from the View > Media Kind submenu. Then choose File > New > Smart Playlist. Set the condition to `[Purchased] [is true]`, click OK, and type a name (such as Purchased) for the smart playlist. Press Return.

No one is going to care that you have only seasons 1–4 and 7–8 of *Buffy the Vampire Slayer,* so don't go into excessive detail here. However, if you plan to leave your media to someone and you know certain items will be particularly interesting to them, feel free to mention them on your list, as in: "…including the first ten Star Trek films and the entire Harry Potter series."

List Other Media

In addition to media you've purchased, you may have music or videos you created yourself, or media that the creator gave away. You may even have some media that you obtained in, um, not-entirely-above-board ways. I'm not here to judge you, but if you have, say, hundreds of hours of shows you downloaded using BitTorrent, it's still important to let your digital executor know what's there. Use the same format as for purchased media—a few bullet items with broad categories—and if the media is somewhere other than your computer (on a media server, say, or a stack of DVDs in your closet), spell that out.

> **Tip:** If there's video of you that exists only online (say, in someone else's YouTube channel), you should at least list the URLs for it. (I'm thinking, for example, of the dozens of video interviews and presentations I've done for various sites. My kids might like to see them, but I didn't create the videos myself, so I don't have copies on my computer.) Better yet, find an app that lets you download those videos to your computer, and include them in your inventory.

An Aside: Digital Media Complications

Earlier, in Understand the Challenges, I mentioned a number of issues pertaining to your digital legacy as a whole, including uncertainty about whether someone in the future will be able to read your digital files because they were in an obsolete format or stored on media that had decayed. While those sorts of concerns apply to all your digital assets, an additional consideration comes into play with media you've purchased, which is that you might not, in fact, own it at all.

Generally speaking, when you pay for software or for music, movies, or TV shows (and, in some cases, ebooks) that can be downloaded or streamed, you aren't purchasing the product as such but rather *licensing* it—that is, you're buying the right to use it. (You know all those license screens you've clicked through without reading when installing apps? That's one of the things they say: "This product is

licensed, not sold….") While you're alive, the legal distinction between licensing and ownership is nearly always abstract. However, the question is what happens when you die. Can the license pass to your heirs, or does it simply expire?

Unfortunately, I can't give you a straight answer to this question, as each licensor is free to specify its own terms—something you'll have to check individually for each party from which you licensed something. (And, if a given licensor doesn't spell out what happens to the license on the death of the licensee—many don't!—you'll have to ask a lawyer.)

Now, you may wonder how a licensor who said your license ends at your death could enforce those terms, assuming they could even discover that you'd died. After all, people sell and give away DVDs, Blu-ray discs, and other physical media all the time, and even though their contents are usually licensed too, this never seems to cause a problem. But the situation is different with most downloadable or streaming media, thanks to the ways they use digital rights management (DRM), a fancy term for copy protection.

DRM is designed to prevent copyright violations by ensuring that only the lawful purchaser of media (such as movies, music, games, and sometimes apps) can use it. For downloadable or streaming media, DRM often means verifying your identity (via a username and password) before letting you use the media. And, some DRM schemes rely on servers that may be shut down in the future, rendering your media unusable—even if you purchased it legitimately and have the files on your computer. (It's happened before!) In practice, then, DRM can make it difficult for you to leave your media to someone else, regardless of whether it's legal to do so.

Note: Apple no longer uses DRM for music tracks that are *purchased* from the iTunes Store, although the company does apply DRM to music downloaded as part of an Apple Music subscription—and to all downloadable video.

Let me walk you through an example based on Apple's iTunes Store (although the facts are broadly similar with most other media sources). Suppose I buy a movie from iTunes and download it to my computer or iPad. I can watch it as many times as I like, but each time I do, my device first checks in with Apple's servers to make sure I've signed in to the iTunes Store on that device with the Apple ID I used to purchase the movie, or one that's part of the same family account (if iCloud Family Sharing was enabled).

In other words, I can't simply give the movie file to someone else and expect them to be able to play it. I *could* leave the person my Apple ID and its associated password, but they can't sign in to both my account and their own at the same time on a given device, and Apple offers no way to transfer purchases from one account to another. So that solution would be awkward at best. (The same logic applies, by the way, if I never actually downloaded the media but only streamed it—say, to an Apple TV. The only way someone else could stream the media I licensed would be to sign in with my credentials, which would mean signing out of their own account.)

The Apple Media Services Terms and Conditions don't explicitly address what happens to the media you've purchased after your death, which means they don't necessarily prohibit you from letting someone else use your Apple ID to access your purchases (awkward though that may be), but they don't necessarily permit it either. (Other vendors may handle the matter in entirely different ways.) In any case, I can certainly imagine scenarios in which, at some future date, Apple might refuse to authorize access to the media from an account whose original owner is deceased.

Ultimately, I can't offer a great solution to this problem, especially given that so many major media providers are themselves vague about their own rules. I do, however, offer a number of suggestions as to how you might approach handing off purchased media to an heir in Handle Your Media.

Inventory Software

I have nearly 300 apps on my computer, and I know people with lots more. Some of them came with the operating system, some were free downloads, and some I purchased. It would be a tedious (and largely pointless) exercise to list every piece of software I own, so I'm not suggesting you do that either.

However, I do think it's an excellent idea to take a spin through your computer's Applications folder and list the software you own in the following categories:

- **Needed to open important files:** Later, in Decide on File Formats, I help you decide what file formats are best for the files you want to leave to future generations. But it may be impractical to export or convert thousands of files right now, and whether you eventually do that yourself or leave it to an heir to do, you'll want to be sure that whoever attempts to access your data after you're gone will have the necessary tools (whether or not they have access to your computer itself). So, if you regularly use any apps that create data in proprietary or rare formats—I'm thinking, for example, of databases; high-end photo, video, and audio editors; virtualization apps; and tools used to compress or encrypt files—make a note of them, along with the name and URL of the developer and the types of documents you use them for.
- **Ongoing subscriptions:** Software that you pay for monthly or yearly—for example, Adobe Creative Cloud, Microsoft Office 365, or 1Password—is worth noting primarily because someone will

need to cancel your subscription (after copying any data that may be stored in the cloud, or moving it to a different account).

- **Apps you want to leave to an heir:** If you've purchased an expensive app whose license terms permit you to transfer it to someone else—and you know of someone who can use it—make a note of the app's name, its license key or code, where the license agreement can be found, and any information you can find (such as a Web page) on the process one must go through to transfer ownership to someone else.

In addition to software on your computer, your mobile devices may also have apps that may be needed to open important files, or for which you have ongoing subscriptions; be sure to list those as well. Because most mobile apps are purchased from an app store (notably Apple's App Store for iOS, or Google Play for Android), and app store purchases are in turn tied to an individual's account and are nontransferable, it is usually not feasible to leave mobile apps to an heir.

Inventory Other Personal Data

You undoubtedly have a great many other files on your computer that don't fit into one of the categories above. It's time to inventory those, but don't panic—when I say "inventory" I don't, in this case, mean you should create an exhaustive index or list. You don't even necessarily have to acquire new organizational habits; after all, organization is to some extent in the eye of the beholder. You do, however, need to take a few steps to help other people understand what you have and how to find it.

Like all children, I hated having my mom tell me to clean my room. It's not that I had any philosophical aversion to tidiness, but the fact was that even though my room looked messy (very, *very* messy!) I knew where everything was. That book I needed for my school assignment? Oh yeah, it's approximately four inches from the top of the

third pile from the left in the northeast corner of the floor. But as soon as I (or my mom) cleaned my room, my organizational scheme broke, and I had to start hunting for every object I needed.

Maybe your computer is the same way. You have files scattered hither and yon, but you know where everything is, so it doesn't matter. And even if you don't know exactly where something is, you know enough about what you have that you can search for a particular file by its name, contents, or other attributes. (The same goes for your email, photos, and so on, each of which may have its own organizational scheme or lack thereof.)

> **Note:** You'll notice that I keep referring to "your computer" here, as opposed to mobile devices. If you use *only* mobile devices, your documents are most likely grouped by app—but apply these same principles to any files you keep in cloud storage (such as Dropbox or iCloud Drive).

Unfortunately, that lack of explicit organization that works fine for *you* might cause serious problems for the people who might need to find something among your digital assets after you're gone.

In particular, the "just search for it" approach is highly problematic when you don't know what there is to search for in the first place! For example, suppose I've written a wonderful short story that's stored somewhere on my computer. I know what the file's name is, and that it's a short story, and that it's worth reading. Even if I don't remember where I put it, I could search for "Raymond's Discovery" and the file would pop right up. But my heirs won't know that I wrote a great short story, what it might be called, or what a randomly found file called "RayDis.rtf" might contain, even if they were to stumble upon it among the million other files on my disk.

Douglas Adams's Hard Drives

When one of my favorite authors, Douglas Adams, died unexpectedly in 2001 at age 49, he left behind a bunch of Macs containing (among other things) numerous drafts of his latest in-progress novel, *The Salmon of Doubt,* which was to be the third in the Dirk Gently series.

A friend collected thousands of files from Douglas's hard drives and sent them to his editor. In collaboration with his family, friends, and others, the editor pieced together as much of the incomplete novel as possible—about a third of the whole story—and included it, along with many of Douglas's essays, articles, and speeches, in a posthumous compilation (also called *The Salmon of Doubt*).

Apart from the 11 more or less complete chapters of the book, all we know about what Douglas intended for that novel comes from a three-sentence description he'd sent to his editor years earlier, and which bears little apparent relationship to what he'd already written.

On the one hand, I was delighted that the material Douglas left behind gave me one last dose of his inimitable writing. On the other hand, he had clearly not arranged his digital affairs in such a way that anyone else could easily imagine what he would have wanted to occur with his data.

Now, you *could* develop an elaborate organizational scheme, creating a detailed hierarchy of carefully named folders or, say, recreating the Dewey Decimal System on your computer. If you have the disposition and the time to do something like that, be my guest.

But in keeping with my "life is too short" mantra, I'd like to suggest a simpler way to inventory your data:

1. At first, don't move any of your files or rename any files or folders.
2. In the inventory portion of your digital will, under the heading "Files," make a list of the major *kinds* of files you have. Don't get fancy, just note general categories, such as:
    - Personal correspondence
    - Financial records

- Insurance information
- Old business documents
- Current business documents
- Unpublished stories
- Receipts
- Random stuff I downloaded
- Miscellaneous notes and snippets

  These are just examples, of course—you'll put your own categories on the list. But if your list goes above 20 items or so, it's too detailed; try combining categories to simplify the list. (By the way, you can skip email, photos, and audio/video media for now; we'll come back to them.)

3. Now, for each broad category, make a few *brief* notes about the sorts of files that category contains. For example, if your category is "School records," you might say, "Homework, term papers, and transcripts from grad school. Master's thesis. Scanned report cards from high school." If any of these file types strikes you as especially significant—something you'd want your heirs to be sure to know about—put an asterisk next to it. (If you're feeling ambitious, you might even list the exact names of a few files that are of unusual importance. But don't overdo it.)

4. Finally, for each category, write a sentence or two explaining how *you* go about finding those files when you want to open them. That could be something like "I go to `~/Documents/Business/Current`" if you're already quite organized, or "I scroll through my Documents folder, opening files that look like potential matches, until I find it," or "I search for words I know to be in the documents, such as (fill in some examples)."

What you've just done is to create an informal annotated table of contents to your files. Notice that you did not move anything, rename anything, index anything, or tax your brain! But this rough guide to your files should give your digital executor, your heirs, and people in the future *something* to go on—a few helpful steps in the right direction of figuring out what you have and where it might be.

Perhaps, though, you noticed in that final step that your answer to where nearly every type of file is was "on my Desktop" or "somewhere in my Documents folder" or "I search for words that only I would think to look for." If those sorts of answers come up often, you may want to refine your organization *a bit*. Creating a handful of folders—perhaps corresponding to broad, top-level categories—and moving the relevant files into those folders (even if each one holds thousands of items) would be a huge help to those sifting through your data later.

> **Note:** Some operating systems let you apply user-defined tags to files and folders, and search by tag. I don't want to discourage you from using that approach if it works well for you, but be aware that years from now, someone might try to find your files while using a different operating system that doesn't recognize your tags. All things being equal, organizing files into folders is a safer long-term strategy.

The bottom line is that the manner in which your files are organized is far less important than your *description* of what you have and where it is. You may organize your files chronologically by year; or according to whether it most closely fits in the animal, vegetable, or mineral category; or alphabetically by the last name of the musician you were listening to when you created the files; and someone else may think that's weird, but an odd-yet-accurate description is way better than "Open every file on my disk and find out for yourself."

> **Tip:** If you use any special, consistent method to name your files or folders–for example, prefixing them with the date created or assigning special taxonomic terms–make a note of that too. Every little clue helps.

You'll recall that I said you could leave email, photos, and audio/video media off your list at first. That's because these kinds of data usually live in their own containers, rather than as separate files—email is in your email app, photos are (often) in an app like Apple's Photos or Adobe Lightroom, and media such as music, movies, and TV shows is (often) in an app like iTunes or Plex.

But now I'd like you to go through essentially the same steps with each of these categories:

- **Email:** Write down a handful of broad categories representing the kinds of saved email you have, and go through the same process to explain the sorts of things each one contains and how you'd go about finding a message of that type. If it seems helpful, you may choose to create additional mailboxes in which to group some of your messages so they're easier to find. But don't knock yourself out; that rabbit hole can go quite deep.
- **Photos:** If you use an app to organize your photos, note which app that is and make a few general statements about how your photos are organized and how you go about finding them. Again, I'm not suggesting that you laboriously label or categorize tens of thousands of pictures; just do your best to quickly highlight anything that's particularly important.

> **Tip:** Many photo management apps, such as Apple's Photos, let you view the date and location where any given photo was taken, and optionally use face recognition to help identify people in your photos.

- **Media:** If your audio and video media (refer back to Inventory Your Media) is in iTunes, Plex, or a comparable app, note where it is and, in general, what sorts of things you have ("13,000 music tracks, 95 movies, and 153 TV shows"). As usual, call attention to anything special that you think someone in the future will want to know about, but don't sweat the details.

Note: Later, in Create a Data Archive, you'll make a copy of (some or all) of your files from your computer onto other media for long-term storage. For simplicity's sake, the files on that media should be organized the same way as on your computer. Don't make extra work for yourself!

Including Someone Else's Digital Legacy in Yours

Suppose your mother dies and, having followed a process like the one in this book, left you with a set of digital documents she wants to pass on. Whether you are her digital executor or merely someone who wants to make sure that data is preserved, you'll want to add her files to your inventory of digital assets. Then you'll include that data with your own in all the remaining steps in this book.

Likewise, it's an excellent idea to ask your digital executor or another family member if they'd be willing to copy your archived data onto their own computer, keeping it backed up along with the rest of their files.

Keeping your data "alive" in this way increases its chances of long-term survival significantly over locking it away separately.

Inventory Digital Currency

The last category of digital asset I'll ask you to inventory is digital currency, if you have any. Unlike cash, or money held in a conventional bank account, digital currency such as Bitcoin typically exists only as cryptographically signed files, often stored in a type of app called a wallet. That is to say, the only record that you own this money may be in a file on your computer, but it's nevertheless a negotiable asset that can be used to buy things or be converted to other currency.

Digital currency (whether in Bitcoin or any of numerous other forms, such as Dogecoin, Ethereum, Litecoin, Peercoin, Ripple, and Ven) should, in fact, properly be listed with your other financial instruments in your conventional will (with clear instructions about how

it should be distributed). Nevertheless, since your computer may provide the only means by which someone can access it, it's wise to include it in your list of digital assets as well. You will need to explain in your digital will exactly how your digital executor can go about accessing (and spending or transferring) your digital currency.

Make High-level Decisions

Pick a door! The decisions you make now will influence how you prepare your digital legacy.

If you've followed the steps in the previous chapter, Inventory Your Digital Assets, you now have a fairly complete list of the items you need to make decisions about. Rather than go through that list item by item, we're going to work our way from larger issues to smaller ones.

In this chapter, I walk you through a number of high-level considerations. First I suggest figuring out the order in which you should attack various parts of the digital legacy process (Determine Your Priorities) and deciding which sorts of stuff, in general, you want to keep or delete (Decide What to Preserve and Discard).

Then we turn to what may be the most important step of all: choosing a digital executor to manage your digital assets when you're gone (Choose a Digital Executor). You'll record your instructions for this person in your digital will, which I described earlier (Begin Drafting Your Digital Will).

Finally, we take a somewhat technical trip into the world of file formats (Decide on File Formats), as I help you decide which file types are best suited for long-term storage.

Determine Your Priorities

The word "legacy" suggests the distant future—the way you want to be remembered generations from now. And, to be sure, preparing your data for the long haul is an important part of the process. However, as you assemble the files and instructions that will comprise your digital legacy, you should think about three time periods simultaneously:

- **The present:** Which of your digital assets could be useful *right now* to your friends, family members, and relatives? For example, would your siblings appreciate having access to your digital photo album? What about the paper photos you'll scan (see Digitize Photos and Documents)—would your relatives like copies too? Are there key passwords you should share with a family member now, to make things more convenient for both of you (see Deal with Passwords)? Could the sorts of instructions you might write for someone to carry out after your death also be useful when you're on vacation next month (see How to Be Me)?

- **Immediate post-mortem needs:** If you die (or become suddenly ill or incapacitated), what digital information would a family member or other trusted person need *right away*? I'm thinking, for example, of access to financial accounts, insurance information, your pre-written obituary (see Your Autobituary), and anything

else someone might need to plan your funeral and make other arrangements in, say, the week following your death.

- **The future:** What digital elements from your life might your children or grandchildren want to see in the next few years? What documents, photos, and other digital data might be interesting or useful years, decades, or centuries from now?

The preparations you make for your digital legacy should encompass all these time periods. However, depending on how much data you have and how you approach the process, it could take you weeks or months to put everything together. What should your priorities be?

There's no right or wrong answer, but I'll offer my own perspective. For me, the sorts of information needed immediately after my death are the most urgent, because I'd want to spare my family as much stress and work as possible if I were to expire unexpectedly. My second priority would be the present, because I'd like to make life better for my family and friends now, and if I didn't get around to archiving everything just so for the distant future, someone else *could* do so later on. But the odds favor me living long enough to handle that too; I'll just make it a lower priority.

In any case, as you go through this book, try to keep all three time periods in mind and make notes for yourself about your own priorities, so you can tackle these steps in the order that suits you best.

Decide What to Preserve and Discard

By the time you've finished this book, you will have thought about a great many digital assets—documents, photos, accounts, and much more. No one has time to ponder the implications of keeping or discarding every last email message, tweet, music track, and every other item in their digital inventory. However, what I do suggest doing at this point is thinking about your digital assets in broad categories

and considering, in general, how much you want to preserve for the future and how much you want to discard (now or after you die).

At one end of the spectrum is a hypothetical person who would like to erase all the digital data accumulated during life—delete every file, erase every disk, close every account, and leave nothing behind. Apart from the fact that it's both practically and technologically infeasible to erase every digital trace of your existence, I'm going to go out on a limb and assume that such a person wouldn't be reading a book about preserving one's digital legacy.

At (or near) the other extreme is where I imagine most of us will be: those who would like to preserve everything. Although a lot of your digital data may boring, redundant, trivial, or poorly organized, keeping everything is much simpler than being choosy. So you'll want to save everything you can, and let future generations sort through it and decide what's interesting or useful. Nevertheless, "save" could mean any of numerous things—for example, do you want your Facebook posts to be preserved *online* or merely saved to a file you can pass on to your children? (I say more about this in Deal with Social Media.)

If you're in between the extremes, you'll need to think about, and take appropriate actions with, data in each category—especially these:

- **Digital photos:** If you want to pass on only a portion of your photo library, you'll either need to discard the rest now or leave detailed instructions about what should be deleted.
- **Email:** Similarly, if there are particularly dull (or incriminating) messages you want to exclude from your digital legacy, such as secret information about yourself or a family member that you would not want to be revealed even after your death, you should find them and either delete them now or put them in a special "Delete This When I'm Gone" mailbox—it's probably too much to ask someone else to figure that out for you.

- **Purchased media:** Do you want someone else to have your collection of digital music, movies, TV shows, games, and other media, assuming it's both technologically and legally possible (see An Aside: Digital Media Complications)? Or do you simply want all that data to be deleted and forgotten?

- **Other files:** What about the thousands of other miscellaneous files on your computer (and mobile devices) or in the cloud—all your letters, financial records, drawings, unfinished screenplays, and to do lists? If there's anything in there you want to expunge from your digital legacy, either do it now or mark it in some way (like segregating it into a "Delete This When I'm Gone" folder).

Unsure which path to take? I'm firmly in the "keep everything" camp, and that's what I recommend. I'd rather spend more time with my children now than waste hours poring through my files trying to figure out what might make them think slightly less of me in the distant future.

Choose a Digital Executor

Part of the process of writing a will is choosing an *executor*—someone you designate to carry out the will's instructions. The executor manages your estate (paying bills, dealing with legal paperwork, handling your finances, and so on) until everything has been settled and your possessions have all been distributed to the appropriate beneficiaries.

Your digital will, too, requires an executor. Your *digital* executor, like a conventional executor, will manage your digital assets until your digital estate is settled. This may include things like answering your email, posting final messages on Facebook and Twitter, closing online accounts, and passing on your digital documents (in the right formats, and stored on the right media) to the people you want to receive them.

In an ideal world, your digital executor and your conventional executor would be one and the same. That would eliminate lots of potential confusion—for example, you have just one person paying the bills that come in the mail and those that show up online; just one person making sure your daughter-in-law gets the dining room table and your son gets your digital photo album.

Like any executor, your digital executor should be a trustworthy person who knows you well, someone you can count on to follow your instructions (and to read between the lines in cases of ambiguity). However, your digital executor needs an additional trait: tech-savviness. You'll potentially be asking them to deal with passwords, Web sites, online forms, backups, file format conversions, and other moderately technical tasks. I don't want to be melodramatic, but I can't overstate this: *your entire digital legacy is in this person's hands*. You want your digital executor to have a great deal of experience and confidence with technology.

In some cases, your spouse or one of your children is a natural fit for this job. If not, try to think of another relative or friend you trust both personally and technically. Or ask someone you trust personally if they can think of someone else with suitable technical expertise.

> **Tip:** If you're drawing a complete blank—there's no one in your life you feel is up to the job—you can potentially compensate for a lack of technical knowledge by spelling out each step, in excruciating detail, in your will. ("Open the lid. Press the power button. Wait until the login screen appears. Type these letters. Press Return." And so on…) Detailed instructions are, in fact, a good idea no matter who your digital executor is, but they're no guarantee of success.

Once you've identified a potential digital executor, talk to them, explain what you have in mind, and make sure they're both willing and able to serve in that role. Then be sure to name this person at the beginning of your digital will (as described earlier, in Begin Drafting

Your Digital Will), and explain both in person and in writing how your digital executor will be able to find the information needed to carry out your wishes.

If your digital executor turns out to be someone other than the primary executor of your will, you *must* make it clear to both people what you expect of them and which tasks will fall to one or the other. These two people will need to coordinate extensively with each other. So I recommend getting together with both of them at the same time, talking through everything, and making sure their respective jobs are spelled out in writing (preferably in both your regular will and your digital will).

> **Tip:** If you're completely unable to find a suitable digital executor—or if you want to hedge your bets in case the person you choose dies or is unable to discharge these duties, you might consider entrusting your data instead to a paid service. See the sidebar Online Digital Legacy Services, much later in the book, for examples.

So far in this chapter, I've talked about relatively general, nontechnical topics. But now I need to switch gears for a moment and discuss a topic that requires a bit more brainpower: file formats. You shouldn't worry if you don't understand everything in this last portion of the chapter, but I wanted to at least acquaint you with the issues so that you—or someone you'll choose to manage your digital affairs—will be able to make informed decisions.

Decide on File Formats

Have you ever tried to open a document you created years ago in an application that is no longer available—perhaps on a platform that itself no longer exists? Sometimes you're lucky enough to find another program that can import that format, or a conversion tool that will translate the old file format into something modern apps can use. But not always. And the more time passes, the greater the chance you'll

be completely unable to open that old file. This has happened to me more than once, and if it's happened during the 35 years or so that I've been using computers, just imagine what it might be like 50 or 100 years from now when one of my descendants tries to open one of my ebooks or some other important document I've made.

We can't know for sure what tomorrow's devices, operating systems, and apps will be like, but we can draw from the last few decades of computing experience and make educated guesses about the future. If you want your files to be readable many years ahead, it pays to start thinking about how you'll store (or export) them right now.

After consulting a variety of sources that deal with archival documents, such as universities, libraries, and historical societies, I've formed some opinions about which file formats are more likely, and less likely, to be readable in the fairly distant future. Basically, my advice boils down to the following principles:

- Avoid proprietary formats in favor of open, industry-standard formats.
- Among open formats, prefer those in wider use.
- Best of all are formats explicitly designed to be future-resistant.

The native file formats used by Microsoft Office (like .doc and .docx) and Apple iWork (.pages, .numbers, .keynote), and Adobe Photoshop's PSD, are prime examples of proprietary formats that were developed and controlled by a single company (even if apps by other companies are also allowed to use those formats). By contrast, PDF is an open format (it was originally a proprietary Adobe format, but was released as an open standard in 2008), as are PNG, TIFF, SVG, and HTML. And the XML format (including XHTML) is, if not future-proof, highly likely to be usable a long time from now because it's encoded as plain text yet structured in an eXtensible way (that's the X in XML) so that it can be adapted endlessly as needs change.

Given those principles, here are my specific recommendations for certain categories of files:

- **Plain text:** Plain text (in either the older 7-bit ASCII encoding or newer UTF-8 or UTF-16 encodings; usually with a .txt extension) is as universal as you can get, and has almost 100 percent certainty of being readable millennia from now. By extension, any file type that's intrinsically plain text but with extra tags or markup (such as Markdown, HTML, and log files) will be at least minimally readable in the future.

- **Formatted text:** Text that has specific fonts, styles, alignment, and other formatting (such as that produced by a word processor) is best stored in one of the following formats, in decreasing order of preference: XML (including .odt), XHTML, or HTML—or, if you're unconcerned about ease of editing, PDF (but see the sidebar PDF vs. PDF/A, ahead). Next best is RTF (a proprietary Microsoft format that is, nevertheless, so widely used as to be a de facto standard). If possible, avoid .docx and especially the older .doc, as well as formats specific to a single app (such as .pages).

> **Note:** OpenDocument, the default format for OpenOffice.org, is an XML-based format for office documents such as word processing documents (.odt), spreadsheets (.ods), and presentations (.odp).

- **Other office documents:** For spreadsheets, use comma-separated text (.csv) and tab-separated text (.tsv) if formatting and graphics are not crucial, or the OpenDocument .ods format if they are. Avoid proprietary formats such as .xlsx, .xls, and .numbers. Similarly, for presentations, use .odp if possible; avoid .pptx and especially .ppt.

- **Scanned documents:** For text-based documents that you scan (see the next chapter, Digitize Photos and Documents), PDF—and, more specifically, PDF/A—is the best choice. See the sidebar PDF vs. PDF/A for more information.

- **Email:** All things being equal, .mbox is the best long-term option. However, .eml and Apple's variant .emlx are also reasonably good choices in that they're based on plain text. Alternatively, you can export email in a more generic format such as HTML/XHTML or PDF. Avoid proprietary formats such as .pst and .ost.
- **Bitmap graphics:** For photographs, digital paintings, and other bitmap graphics, prefer TIFF, PNG, and JPEG2000 (in that order). (Bitmaps can also be embedded in PDF documents.) Avoid using .bmp and GIF. And, although conventional JPEG (with lossy compression) is the most common format for today's digital cameras and will probably be readable in the distant future, it's still a less good choice for archival use than any of the uncompressed bitmap formats.

> **Note:** Many cameras, especially DSLRs, store raw images instead of (or in addition to) JPEGs. Although raw images are great in terms of fidelity, the wide variety of raw formats (and the fact that photo editing software must constantly be updated to accommodate raw images for new cameras) makes raw images unsuitable for archiving.

- **Vector graphics:** Your best choice is SVG. (Vector graphics can also be embedded in PDF documents.) Avoid .ai/.ait and EPS if possible.
- **Audio:** Use WAV, AIFF, FLAC, or OGG if possible. Although MP3 and AAC (.mp4) are also good formats in wide use, they're less future-proof. Avoid .wma.
- **Video:** Prefer AVI or QuickTime (.mov) without compression, or Motion JPEG. Next best are MPEG (.mpg/.mpeg) and MPEG-4 .mp4, although their future is less certain. Avoid .wmv.
- **Compression:** All things being equal, the safest approach for long-term viability is not to use compression at all. If you must compress files, ZIP format is the most universal.

Tip: If all these initials are making your head spin, don't fret. All I'm saying is: given the choice, it's preferable to save files in formats that are more likely to be readable a long time from now. If you need help figuring out the mechanics of saving, exporting, or converting files, your digital executor can probably help.

PDF vs. PDF/A

PDF is one of the most widely used file formats for ebooks, instruction manuals, academic papers, scanned documents, and just about any other type of file for which the creator wants to ensure that formatting is preserved regardless of the platform or app used to display the document. It's a good long-term format for nearly any type of text or graphics document, although it's not as easily editable as, say, XML.

There are, in fact, numerous versions of PDF. One of them—PDF/A—is designed specifically for archiving. Any app that can open conventional PDFs can also open PDF/A documents. However, PDF/A documents have special metadata that identifies them as such, and they exclude elements that may be present in regular PDFs but are not suitable for long-term archiving, such as:

- Externally linked content (such as fonts and graphics)
- Audio and video
- JavaScript
- Encryption

A regular PDF document that avoids these elements is, for all practical purposes, just as good as a PDF/A document—but it can be difficult for a layperson to tell whether a PDF meets those criteria. You can convert PDF to PDF/A with apps such as Adobe Acrobat Pro DC and PDFpen (Mac only), or online tools such as docuPub.

Once you've decided on which file formats to use, then what? If you already have zillions of files in formats that are unsuitable for archiving, what should you do?

Well, for one thing, you'll want to keep your preferred formats in mind as you Digitize Photos and Documents, Deal with Email, and Deal with Other Digital Data. And, in some cases, you may want to export or

convert your data to a more suitable format when you Create a Data Archive. In the meantime, however, you can use this information in a few ways:

- If you regularly use apps (such as word processors or graphics tools) that give you a choice of file formats, and you can opt for a format that's better suited to long-term storage for future files you create, begin doing so. (For example, if your word processor lets you choose between .doc and RTF, go with RTF; if your photo editor lets you choose between JPEG and TIFF, go with TIFF.)
- Time permitting, you might convert your existing files in batches, perhaps starting with the documents that you feel are most crucial to preserve for long-term accessibility. Software that can do these conversions in batches is generally available, depending on what you want to convert to what. For help, ask a technically savvy friend or a computer consultant, try a Google search, or even explore this question with your digital executor.

> **Note:** With photos, be aware that there is a huge trade-off in file size between JPEGs and uncompressed TIFFs—if you convert your images to uncompressed TIFF format, they will take up much more space. However, according to experts in archival storage, relying on formats like JPEG that include compression makes your photos considerably less likely to be readable in the distant future. If you are put off by the amount of effort or storage space that would be required to convert your photos to uncompressed TIFFs, your JPEG originals are far better than nothing. But you might suggest in your digital will that your heirs revisit that decision from time to time, as preferred file formats change and storage inevitably becomes cheaper.

- If the thought of converting all your existing files to better formats is likely to drive you to an early grave, consider assigning that job to your digital executor—or see if you can draft a tech-savvy child, grandchild, neighbor, or friend to help you out.

File Formats: Other Opinions

Lots of people and institutions have researched the topic of which file formats are most sustainable. They don't always agree with each other (or with me), but if you're interested in seeing other opinions and the reasoning behind them, check out these sources:

- Digital File Types at the U.S. National Archives (see also Appendix A: Tables of File Formats)
- File Formats for Archiving (PDF) at ETH-Bibliothek Zurich
- Format Conversion Strategies for Long-Term Preservation at the University of Michigan's Bentley Historical Library
- Electronic Records Management Guidelines at the Minnesota Historical Society
- Recommended File Formats at Virginia Tech's Digital Library and Archives

Digitize Photos and Documents

Many of us have boxes full of old photos and documents that will last longer if converted to digital form.

If you're like most people, you have photos and videos in digital format going back to whenever you started using a digital camera. You probably also have digital documents of various kinds stretching back even longer. But you may also have paper photos from earlier decades in albums or shoeboxes, not to mention paper documents that may have historical or sentimental value—school records, old love letters, your recipe collection, and so on.

Of course, you can (and probably should) leave those boxes of paper to your heirs. But paper deteriorates over time and is also subject to the damaging effects of moisture, heat, and other environmental issues (not to mention fire, flood, and so on), so if you want that material to be preserved indefinitely, making a digital copy is an excellent idea. Doing so also enables you to make those photos and documents more easily searchable and sharable, benefits you may well take advantage of right now.

The effort and expense involved in scanning these photos and documents is largely a function of quantity—it's no big deal for a handful of pictures, but scanning tens of thousands of pages could take you years or cost a great deal of money. In this chapter, I spell out various ways you can tackle this task, discuss the ways the digital files should be organized and preserved, and help you consider various options for handling the original paper copies.

> **Tip:** As useful as it is to digitize your paper photos and documents, I consider this a lower-priority task than preserving data that started out in digital form. After all, someone else *could* deal with the paper later if need be. So, if you get partway through this chapter and start feeling like this part of the process is too overwhelming, my advice is to skip it and return to it later if you have the time and energy.

Take Preliminary Steps

Whether you're looking at a single folder full of pictures or a huge stack of boxes, each with thousands of pages, your first step should be to take stock of exactly what you have and what your priorities are. There's no right or wrong way to approach this, and every situation is a bit different. I'll sketch out my basic suggestions, which you can adapt to your own needs:

- **Separate the wheat from the chaff:** Not every photo or document is worth preserving in digital form for posterity, and the more you

scan, the more time or money you'll spend. So, as a first pass, I recommend separating all your paper photos and documents into two piles (or boxes or whatever): those you consider important to digitize and those you don't.

I can't tell you exactly what criteria to apply in making this decision for your own stuff, but I know I'd prioritize pictures of people over pictures of places and things, and pictures of people I know over those of people I can't identify. Given several similar photos, I'd choose just my favorite, or the one that's clearest and sharpest.

- **Sort by type:** Each type of media (photographs, slides, and documents) needs its own pile. I would further sort photographs into subcategories, such as:
  - *Ordinary photos:* Photos, in good condition, printed on thick photographic paper
  - *Mounted photos:* Anything that's framed, matted, glued into a photo album, or otherwise attached to something larger
  - *Delicate photos:* Photos on thin or fragile paper (such as newspaper clippings), those that are physically deteriorating, or anything that might require special care when handling

  In addition, anything larger than roughly legal size, plus anything that's not flat or that for some other reason might not fit in an ordinary scanner, should get its own pile (see What about Large, Irregular, and 3D Objects?).

- **Sort by date:** If you already know (even approximately) when each photograph or document was created, sorting each pile by date can be helpful because it will simplify the process of naming and organizing the scanned files later. If you don't know most of the dates, or if it's too much effort to think about it now, you can skip this step for now and come back to it when you have the digital files.

- **Sort by priority:** If you are looking at 20 knee-high piles of photos on your living room floor, all part of your set of photos that you consider important to digitize, you might find some comfort in one last sorting pass. For each pile, divide the items into two or three sets—for example, those that are crucial to your digital legacy, those that you'd really like to scan if reasonably possible, and those that could be dealt with at some point but aren't that important.
- **Count:** Count the number of items (or pages) in each of your piles or categories. You don't need an exact number; "around a dozen" or "two hundred-ish" is close enough. (If your piles are quite high, you can count how many items are in an inch or centimeter of depth and then use a ruler to approximate the total.) Having a count will help you estimate how long the scanning will take if you do it yourself, or how much it will cost if you pay someone else to do it for you in a way that "7 big ol' boxes" or "12 kilograms of photos" would not.

Again, these are all just suggestions. You might find it makes more sense to sort by priority first, and then by date; or to do a single sorting pass in which you sort your photos every which way. But what you should end up with is several groups of photos and documents, which you can then tackle one at a time.

Digitize Other Media

This chapter is all about still photographs and static documents, but you may find other media with great historical or sentimental significance that you'd like to preserve for the ages, too, such as:

- Audio tapes (such as reel-to-reel, cassette, or 8-track)
- Vinyl records (or even older discs or cylinders)
- Videotapes and videocassettes
- Movie film (8 or 16 mm, Super 8)

All these media can also be digitized, and I strongly recommend doing so. Again, you can buy the necessary equipment to do it yourself, but the prices are often prohibitive and digitizing audio and video may require more technical expertise than scanning photos. A better bet is to outsource the work. Many companies offer such a service; in a quick Web search, I found the following examples:

- Analog-to-Digital.net
- iMemories
- SEADS Analog to Digital Services
- video4u

Scan Photos and Documents Yourself

Scanning photos and documents yourself isn't complicated, although it does involve an investment of money and time.

If your items have unusual sentimental value, or are extremely fragile, and you're nervous about shipping them off to some company across the country to handle (see Outsource Scanning), scanning them yourself is certainly the right move. You might also do the scanning yourself if you have plenty of time and you determine that the cost of a scanner is much lower than the cost of paying someone else. (For example, if you're comparing a service that charges $0.60 per scan with buying a $150 scanner, the break-even point is 250 photos.)

Tip: As a way of economizing further, a family member or friend may have a scanner you can borrow, or may be willing to do the scanning for you in exchange for one of your world-famous cherry pies. Just food for thought—I mean, food for scan.

Obtain a Scanner

If you're going to scan photos or documents yourself, you'll need a scanner! Scanners come in all shapes and sizes, but most fall into one of the following two categories:

- **Flatbed scanners:** This type of scanner (such as the Epson Perfection V550) operates much like a photocopier: lift the lid, place your photo or document face down on the glass, and press a button (on the scanner or in an app). A few seconds later, the scanned image appears on your computer's screen, where it can be saved as a TIFF, JPEG, or other graphics file.

  Flatbed scanners typically have much higher resolution than document scanners (for example, 6400 dpi resolution is not uncommon for a flatbed, whereas document scanners typically top out at 600 dpi). Flatbeds can scan book pages and other items that are thick or rigid, whereas document scanners can't. Some flatbed scanners include an attachment that will let you scan slides. On the other hand, flatbed scanners are much slower and require more manual interaction than document scanners.

- **Document scanners:** Designed for digitizing documents such as letters, reports, business cards, and receipts, document scanners (like the Fujitsu ScanSnap ix500) usually feature an upright design with an automatic sheet feeder. Put a stack of pages in, press the button, and watch as 20 or more sheets per minute zip through—usually scanning *both* sides of the page in a single pass. These scanners generally save documents as PDFs, with the option to apply OCR (optical character recognition) so that you can later search your scanned documents by content.

Document scanners are faster and more convenient for scanning large numbers of pages. They're fine for most photos, too, as long as the photos are sturdy enough to survive a trip through the sheet feeder and you don't need super-high resolution. (If in doubt about the robustness of an old or delicate photo or document, however, don't take a chance on using a sheet feeder.) But you can't use them to scan slides, books, passports, matted photos, and other extra-thick items.

Note: Most scanners hook up to a Mac or PC. Some scanner models can connect to a Wi-Fi network and send scanned images directly to cloud storage (such as Dropbox or Evernote), and that's a feature you may want to look for if you use only mobile devices. But, generally speaking, you'll have more control and an easier time processing images when you use a scanner attached to a computer.

I've used document scanners for years to scan mail, tax documents, bank statements, contracts, and other documents; I've also used them for snapshots and other photos. By using a *carrier sheet* (basically, two thick sheets of clear plastic joined at one end), I've also scanned delicate and irregularly shaped items that the rollers might otherwise have scrunched into oblivion. If you have more documents than photos to scan, or if your photos are mostly of a sort that will fit in a document scanner, a document scanner is probably your best choice.

On the other hand, if you have more photos than documents; if you want to scan photos at a very high resolution to bring out as much detail as possible; if you have lots of thick or irregular items to scan; or if you want to save money (since flatbeds tend to cost less than document scanners), a flatbed might be the way to go. (Of course, you're welcome to buy one of each, if you can afford it!)

The last time I owned a flatbed scanner was about 15 years ago, so I don't have enough recent experience to recommend a specific model or brand. If I were in the market for one, I'd read reviews on Amazon and pick something that's highly rated but not terribly expensive.

If you opt for a document scanner, I can tell you I've owned several Fujitsu ScanSnap models, and have been happy with all of them. For more options, consult the online appendixes for my book *Take Control of Your Paperless Office*, which contain tables comparing a great many models from a variety of manufacturers.

About Google PhotoScan

A scanner is basically a fancy digital camera. If you were to position a regular camera carefully over a document, with optimal lighting, and take a picture, you could get essentially the same result. But if you've ever tried this yourself, you have probably discovered that the positioning and lighting are, in fact, incredibly difficult to get right! Photographs of documents and other photos nearly always look a lot worse than scans of those same items.

Some smartphone apps, however, claim to solve this problem. Most notably, Google PhotoScan (available for Android and iOS) walks you through the process of taking multiple snapshots of a paper photo. It then stitches them together into a single image and applies some heavy-duty math to straighten it out, remove glare, and otherwise improve the image quality. The effect is supposed to be similar to running the page through a scanner—but all you need is the smartphone in your pocket and a free app. What's not to like?

I've tried PhotoScan, and although I had high hopes, I wasn't pleased with the results. I found the images to be lower in resolution, of poorer overall quality, and in greater need of manual fiddling, than images made using a scanner. Several other reviewers have said much the same thing about the app. In other words, it's a neat idea, and better than nothing, but you get what you pay for—it's not a substitute for a real scanner.

Other apps, such as Microsoft's Office Lens for Android and iOS, offer similar capabilities but without the essential glare-removal feature. They're pretty good for documents, but not ideal for photos.

I wouldn't be surprised if apps of this sort get much better over time. Perhaps they'll eventually eliminate the need for scanners. But in my opinion, they're just not there yet.

Scan Photos and Documents

Once you have your scanner, you'll need to hook it up, install any included software, read the instructions, and start working your way through your piles of photos and documents.

I wish I could offer you detailed, step-by-step directions, but the steps will be completely different depending on which type and model of scanner you use, which operating system your computer runs, which software your scanner includes, and your personal preferences. I can, however, offer you a few tips:

- **Find the right resolution:** Regardless of what type of scanner you use, you can choose a lower or higher resolution (number of dots per inch) for your scans, up to the maximum the scanner supports. Higher resolutions give your scanned images more detail, but the higher the resolution, the longer the scan will take and the larger the resulting file will be. And, if your original photos aren't quite sharp and detailed, an extra-high-resolution scan won't make them look any better than a lower-resolution scan. So the trick is to find the lowest resolution that yields acceptable quality given your source material.

  In my experience, when scanning photos, 600 dpi usually provides the best compromise among quality, speed, and file size. For documents, 300 dpi is usually ideal when scanning in color or grayscale, but 600 dpi is better when scanning in black and white. My suggestion is to scan a few photos and documents at each of a few resolutions—say, 300 dpi, 600 dpi, and 1200 dpi. Notice how long each scan takes; then examine the resulting images on your screen carefully, compare their quality, and take note of how large the files are. Then decide on the setting that works best for you. (You can, of course, choose a higher or lower resolution setting for certain images and documents if you prefer.)

Tip: Most scanning software also lets you choose whether to scan in black and white, grayscale, or color; and, for color, the bit depth (higher numbers mean a broader range of colors). For most photographs, a 16-bit color setting (even for black-and-white originals) is about right, whereas most documents will do best in grayscale.

- **Choose the right file format:** Your scanner will almost certainly provide several choices of file format. You may be tempted to choose JPEG, which will usually produce the smallest file sizes, but JPEG compresses images in a way that removes information—not the best idea for archival use. As I said in Decide on File Formats, your best option for photographs is TIFF—preferably *without* compression—but PNG is a good second choice; for scanned documents, PDF (preferably PDF/A) is the way to go.
- **Let your scanning software help:** Most scanners include software with settings that enable it to automatically deskew crooked images; crop images so that the files contain only the photo itself (and not the border or a bunch of extra white space); and apply other image enhancements, such as color correction. Experiment with these settings to find what works for you, but to the extent possible I suggest letting the software do these tasks rather than manually fiddling with each and every image.
- **Get extra help with document scanning:** If you'd like to learn much more about the ins and outs of document scanning in particular—including dealing with OCR and managing lots of scanned documents, check out my book *Take Control of Your Paperless Office*.

It may take you a while to find your groove and get to the point where you can process photos and documents efficiently. But you should eventually be able to do scan about one photo per minute, from start to finish. (You'll go even faster with simple, multi-page documents if you use a document scanner with a sheet feeder.)

> **Tip:** If a photo has writing on the back, I suggest scanning both sides. Your computer will save them as two separate images, but this information can be helpful in identifying dates and subjects later on.

Regardless of the scanner and software you use, you'll have to decide how you want to name, organize, and store the scanned images. I discuss all this ahead in Name and Organize Digitized Files. First, however, I want to say a few words about an alternative to scanning your own images: paying a company to do it for you.

Outsource Scanning

If the idea of buying a scanner, figuring out the software, and scanning thousands of photos fills you with dread, you might want to consider outsourcing the task instead. Numerous companies let you mail them a box of photos, slides, and/or negatives; they then do all the heavy lifting of scanning them and enhancing the digital images, provide the final product (as downloadable files; or on DVD, CD, a flash drive, or a hard drive) for well under a dollar per photo, and mail back your originals.

The Wirecutter undertook an extensive review of dozens of scanning services and compiled the results in The Best Photo Scanning Service. Their top recommendations charge between $0.39 and $0.60 per photo, although in some cases you'll pay an extra hourly fee if you want the service to provide manual photo retouching. The article details what you can expect in terms of timing, quality, and customer service from various providers. I have no personal experience with any of these companies, but if I were looking for a company to provide this service, I'd most likely go with The Wirecutter's top pick, Memories Renewed.

The services listed in that article primarily handle photos, not documents. Although numerous companies scan documents, perform OCR, and turn them into PDF files, nearly all such services are geared

exclusively toward businesses, and at least two companies that used to offer consumer-oriented document scanning have stopped doing so in the last year or two. However, you can often find business centers (such as FedEx stores) that offer either do-it-yourself or staff-assisted scanning services, and if you have only a small number of documents to scan, that might be a cost-effective choice.

Name and Organize Digitized Files

If you scan photos yourself, your scanning software will most likely give your files default names based on the current date and time, for example `2017_01_09_21_51_00.tiff`. Or it may, like your digital camera, give the files sequential numbers, like `IMG_01234.png`. Those sorts of names, by themselves, are nearly useless, as they tell you nothing whatsoever about the file's contents.

On the other hand, manually choosing a name for each file that's both descriptive and readable is a lot of work, and will leave you with hundreds of files with lovely names like `1974-November-Aunt-Ethel-station-wagon-in-front-of-Florida-house.png`. Ugh. And furthermore, if you put all these photos in an app like Apple's Photos or Adobe Lightroom, you may never even look at the filenames themselves—you'll either identify photos visually or rely on albums, tags, or other methods of categorizing and labeling them.

I like to keep things simple, but I also like to provide myself (and anyone in the future who may look at my photos) enough information to be at least minimally helpful. So, allow me to suggest the approach used by my friend and colleague Marshall Clow, who has scanned many thousands of family photos: number your files sequentially (`1000.tiff`, `1001.tiff`, and so on) and describe them in a separate, annotated index.

Yes, I said just a moment ago that sequential numbers, by themselves, are useless. You can make them useful, however, by creating a simple

text document that lists each numbered filename along with a brief description. You can then search in that document (by name, date, or whatever other notes you include) to locate any given image. If you go this route, observe these tips:

- As you scan photos, look at them carefully and include items such as the following in your notes:
  - Whatever you know about the photos, such as the approximate date, location, and names of anyone in them
  - Any text printed on the photos themselves, including photographers' stamps
  - Anything handwritten on the front or back of the photos
  - Comments people have made about a picture, along with who said something and when; be sure to distinguish facts from opinions
  - Questions you have about the photos (such as "Why is Uncle Ted missing from this photo of the family reunion?")
  - Information relating to other photos (for example, in the notes for photo `1234.tiff`, you might say, "I'm pretty sure this was taken at the same time as `1108.tiff` and `1336.tiff`.")
- Be careful that your scanning software doesn't arbitrarily restart the numbering (for example, after a system crash or other glitch); otherwise, you'll end up with a confusing set of duplicate filenames. In fact, even if your software offers to number files sequentially by itself, you may want to number them manually.
- To avoid the clutter and confusion of thousands of image files in a single folder, consider dividing your images into folders of 100 or so photos each.

- If you've scanned both the front and back of a photo, give the two files matching names—for example, `1234-front.tiff` and `1234-back.tiff`.
- If you crop or otherwise edit a scanned image, make the modifications on a *copy*, and *always* leave the original file intact.
- Keep your annotated index in a safe and easily accessible place.
- Take your time, and don't worry about finishing quickly. It's better to scan and annotate a small fraction of your photos than none at all.

Integrating Old and New Data

Should you mix all these photos you're scanning in with your existing digital photos, perhaps by adding them your photo album app but keeping them segregated somehow? Or should you keep them isolated as entirely separate digital files? This is entirely a matter of personal preference, but my feeling is that keeping all your digital photos in one place (including those that were originally analog) is the simplest approach.

And remember, a century from now, no one will care which photos you snapped with a digital camera and which you scanned. They'll just want to see the pictures!

Back Up Digitized Files

In a sense, the entire project you're undertaking amounts to making a backup of all your important data, which you'll store in a secure, permanent way. However, in the meantime—while you're still alive, and especially in the weeks or months before you've finished digitizing all your old photos—it's important to make regular backups of everything. You would not want to lose all that work to theft, fire, or another catastrophe.

If you already back up the other files on your computer, the ones you're creating now should automatically join your existing backups. If you don't already have backups, there's no time like the present to start.

I've written several books on the topic of backups and I don't want to go into a great deal of detail here. I do, however, want to suggest strongly that at the very minimum, you have two kinds of backups:

- A copy of all the data from your computer, stored on an external hard drive and updated at least weekly (although daily or even hourly is even better); this makes your backup easily and quickly accessible.
- A second copy of all your data, stored somewhere else (on a second hard drive that you rotate to another location, or in a cloud backup service such as Backblaze or CrashPlan); this provides insurance against any sort of disaster that takes out your local backup.

If you're looking for additional advice, opinions, or suggestions, I can recommend two things I've written:

- My article The Best Online Backup Service at The Wirecutter discusses a number of online backup services in detail and says the best options for most people are CrashPlan or Backblaze.
- My book *Backing Up Your Mac: A Joe On Tech Guide* is a comprehensive guide to backups for Mac users.

Decide What to Do with the Originals

Once you've scanned your old photos and other documents, what should you do with the originals? Once again, the answer is up to you (and it may vary from one photo or document to the next), but in general, I urge you to keep them—and even redouble your efforts to preserve them—even though you've scanned them.

My computer contains scans of 50-year-old (and much older) photos, and I love having them there because I can search them, post them on Facebook, send them to family members, and put them to other uses that aren't possible with that lone, fading paper copy. One day, those digital copies will be all that's left, and I (or my distant descendants) will be grateful to have them.

And yet, even though everyone has seen a photo of the Mona Lisa, the original still draws huge crowds every day at the Louvre. There's something about holding (or at least seeing, in person) an actual old object that is much more meaningful than merely seeing what it looked like. Chalk it up to irrational human nostalgia if you will, but I like the fact that I not only know what my father's high school grades were in 1939, I have the original report cards too! Other antique items, such as ticket stubs, theater programs, and diaries, likewise, may not have any commercial value, but they certainly have sentimental value and I'd like to preserve them as long as possible.

If you have strong anti-packrat tendencies, and your family is in agreement, there's no legal or ethical prohibition against tossing (or recycling) your old photos and documents once they're scanned. But I urge you to preserve the originals if at all possible; remember that one person's trash is another person's treasure. (See Don't Let Your Family History Be Tossed in the Trash, by Thomas Jay Kemp at GenealogyBank, for a fine example.)

Assuming you decide to keep the originals, I suggest the following:

- Geometry permitting, put each photo or document in an acid-free polypropylene envelope, which will protect it from scratches, skin oil, and other potential causes of damage.
- Label each item's envelope with the filename you gave its digital counterpart.

- Store the photos and documents in roughly the same order and groupings as their corresponding digital files, and labeling them (at least by box or envelope) each group (for example, in a box or large envelope) so that someone in the future can match the originals with the digital versions.
- For maximum longevity, keep your original photos and documents in a cool, dry, and dark place—an opaque, airtight plastic box stored in a closet, for example.

What about Large, Irregular, and 3D Objects?

Among the papers you want to preserve, you may find mounted photos that can't be safely removed, plus posters, paintings, oversized photos, collages, and other objects that either aren't flat or won't fit in or on your scanner. Until consumer-grade, full-color, high-resolution 3D replication becomes affordable, I can make a couple of suggestions:

- If the item is flat but oversized, you may be able to borrow, rent, or pay to use a large-format scanner at an office supply store, graphic design firm, or print shop. I've seen scanners that can handle media at least 36 inches wide.
- Although 3D scanning exists, it's not yet available in a form that's particularly convenient, affordable, or usable for most consumers. As an alternative, photograph the object from every possible angle (preferably without a flash, to reduce glare) and preserve both the photos and, if possible, the original object.

Deal with Passwords

Every site and service that asks you for a password represents information you need to pass on to someone.

When I turn on my computer, it asks me for my password; without it, no one would be able to access any of my files. The same goes for my smartphone and tablet (although mobile devices typically use shorter, numeric passcodes). And in the course of my work and play, I use (at least occasionally) hundreds of Web sites, apps, and cloud services,

each of which requires an account with a username and password, and most of which contain at least some information that would be interesting or useful to my family and friends when I'm no longer around.

In fact, "useful" is an understatement: without access to certain accounts, no one will be able to carry out my wishes—whether that means shutting them down, preserving them for posterity, or keeping them going under new ownership.

You should already have a list of your most important accounts (see Inventory Online Accounts). Whether you have just a handful of accounts or thousands, and whether you consider the information in them to be trivial or essential, you should take steps to ensure that the accounts are accessible to your digital executor—and that you've clearly stated what you want to be done with them. In this chapter, I discuss how to go about doing that.

Use a Password Manager

I've spent much of my writing career urging readers to protect themselves, their data, and their online privacy in various ways—backups, encryption, secure Web browsing, and so on. One of my most important recommendations, which I've come back to time and time again in books, articles, presentations, and courses, is to be smart about the way you use passwords.

If you'd like all the details on improving your password security, you can read my book *Take Control of Your Passwords*. But let me just offer a few key pieces of advice from that book here:

- Don't reuse the same password for more than one site or service, no matter how inconsequential you think the account is.
- Choose passwords that are long, random, and contain a mix of uppercase and lowercase letters, digits, and punctuation.

- Use a password manager app (such as 1Password, LastPass, or Dashlane) to generate, store, and fill in passwords for you.

Password managers don't solve every password problem, but they do make it incredibly easy to be safe. You choose a single, strong master password that will unlock your password manager, and that becomes the only password (or, realistically, one of just a few) that you need to remember.

So, if you don't already have excellent (strong and unique) passwords, this is a good time to think about changing your habits to protect your data for yourself and for your heirs—and a password manager makes that process as painless as it can be.

> **Tip:** I wrote an extensive comparison of The Best Password Managers for The Wirecutter.

For the purpose of this book, a password manager serves another essential function: It provides a repository of all your accounts and their credentials, so your digital executor knows what accounts you have *and* how to access them. In other words, it simplifies your digital will; you need not provide a long list of accounts and passwords, but rather just access to your password file and the master password that unlocks it. (In fact, there may be an even better way to give your digital executor access to your password manager, as I discuss ahead in Give Your Digital Executor Access to Your Passwords.)

If you have hundreds of accounts that all use the same password—or that use different but weak passwords—the process of changing your passwords and moving all that information into a password manager could take a while. In my personal and professional opinion, it's well worth the time and effort. But in the meantime, at least create a simple password list (see the following sidebar) to include in your digital will; something is better than nothing.

A Simple Password List

If you have a relatively small number of accounts (say, a dozen or two), you may justifiably feel it's not worth the hassle of setting up a password manager. If so, there's nothing wrong with a paper list of your accounts with their usernames and passwords.

Likewise, if you have only a few passwords for many accounts, writing them down is a reasonable interim measure. Yes, you *should* change them all so they're unique and store them in a password manager, but since that could take a while, a paper list is far better than nothing.

I do want to stress, however, that keeping your written password list next to your computer or otherwise in plain view is unwise. Choose a safe location—somewhere your digital executor will be able to find it but a thief won't.

Highlight Key Accounts

Of the nearly 900 accounts in my own password manager, only a handful contain (or provide access to) information that would be crucial to my digital executor in the days after my death. For example, my bank accounts, insurance accounts, email accounts, Dropbox account, and social media accounts might all require immediate attention for one reason or another, whereas there's no urgency for my accounts for frequent flyer programs and online discussion forums to be shut down.

You will know better than anyone else which accounts are likely to require timely action, and you can reduce your digital executor's stress considerably by making a note of which accounts those are. So, take a few minutes to scroll through your list of accounts and identify those that fall into these categories:

- **Email:** Access to your email accounts is crucial if your digital executor is to manage your other accounts and handle a variety of other details for you. (See Deal with Email.)

- **Social media:** You may want your digital executor to take action of some kind with your Facebook, Twitter, and other social media accounts—posting a final message, for example. (See Deal with Social Media.)
- **Money:** Any account that involves money—banking, investments, insurance, utilities, PayPal, and so on—may be important for both your digital executor and the executor of your conventional will (if they're two different people).
- **Key documents:** Medical, financial, and other records that exist only in online accounts may need special treatment, and the accounts themselves will usually need to be closed (although in some cases it may be better for ownership to be transferred to someone else).
- **Cloud storage and backups:** Services that store your files in the cloud in one form or another (Amazon Cloud Drive, Backblaze, CrashPlan, Dropbox, Google Drive, and many others) should be readily available to your digital executor. (See Handle Other Cloud Data and Handle Backups.)

Most password managers offer one or more ways to label or categorize accounts. For example, 1Password lets you apply user-defined tags to any item, and LastPass lets you organize logins into folders. Whether you use the tools built into your password manager or even write a simple list, make it obvious which accounts your digital executor needs to pay attention to, and include in your digital will a note about how you've identified those items.

Also include in your digital will detailed instructions for any accounts that need special consideration. Your digital executor will probably close most of them eventually, but if you want to pass an account on to someone else or take some other action that wouldn't otherwise be obvious, be sure to write it down.

Give Your Digital Executor Access to Your Passwords

I said earlier that you *could* simply provide your digital executor with access to your password file and your master password. For example, you could include your master password in your digital will along with the location (on your computer or elsewhere) of the file containing your passwords. Although that will usually work, I'd like to suggest two alternatives that are both safer and more flexible:

- **Emergency access:** A number of password managers, including LastPass and Dashlane, enable you to set up emergency access to your passwords for one or more specified people. When a person on your designated list requests access and a predetermined length of time passes, they're granted access to your passwords (or a selected list of passwords).
- **Shared folders or vaults:** LastPass lets you set up a folder, put whatever passwords you like in it, and share it with up to five people. 1Password provides a number of methods by which you can securely share a *vault* (1Password's term for its secure storage files) with someone else—you can either put a vault in a shared Dropbox folder or use a 1Password Families account (if your digital executor is in your family) or a 1Password Teams account (if your digital executor is in your company). A number of other password managers offer comparable features.

In all these cases, if you change a password, the people with whom you're sharing your passwords always see the latest version, which is obviously not the case if you simply write your current password on a list—and they never need to know your master password. The other nice thing about shared folders or vaults in particular is that you can give a family member access to certain passwords now—that can be handy for accounts you and your spouse need to access, for example.

Note: Be aware that when you give someone else access to your passwords, you're giving them a *lot* of power. They can log in as you, change your password, copy or delete private data, and so on. I can't emphasize strongly enough that you should share your passwords only with someone you trust implicitly—keeping in mind that this person will have the ability to use your passwords while you're alive.

Regardless of how you choose to give your digital executor access to your passwords, make sure there's a "Passwords" heading in your digital will and, underneath it, spell out exactly what your digital executor needs to do to get in to your accounts.

Whether or not access to your password manager's data file also requires access to your computer or mobile device, make sure you include the password or passcode to all your computer(s) and mobile device(s) in your digital will. They might be redundant if they're also in your password manager, but because they're so important, it doesn't hurt to have that extra insurance.

Warning! If any of your accounts use two-factor authentication or two-step verification, you'll need to include detailed instructions as to how your digital executor can obtain the extra codes needed to unlock them. For example, if codes are sent to your cell phone via SMS, you'll need to ensure that your digital executor has your cell phone and its passcode—and knows to keep paying your monthly cellular bill for as long as such messages may still be needed.

Deal with Email

Your stored (sent and saved) email can tell future generations a great deal about you.

Some people treat email as an entirely ephemeral means of communication, along the lines of telephone calls. They receive a message, reply to it (or not), delete it, and then never think about it again. At the other end of the spectrum are people like me who save virtually every email message they've ever sent or received. In between are

numerous other strategies for handling email, but I think it's fair to say that most of us have some quantity of saved email, and it may turn out to be one of our most important digital assets.

Without a doubt, a large percentage of email we send and receive is unexciting (to say the least). And yet, a trip through my email archive can tell me (or someone else) things like:

- Where I traveled and when
- What I purchased and when
- Extensive details of work and personal projects
- How I reacted to important events in my life and others' lives
- When I set up various online accounts

And, of course, much more. This information could be incredibly valuable to your heirs, even though it may take extensive searching and filtering to find the useful tidbits.

On the other hand, I know people who, for the very same reasons, want to make sure no one else can ever see their email! Maybe it contains secrets you want to remain secret forever, or maybe it shows an embarrassing side of you. Whatever the reason, if you want to *avoid* letting other people access your email when you're no longer around, that, too, will require planning.

There's also the matter of ongoing email access. If you get hit by a bus tomorrow and an old friend (or coworker, or business) sends you email next week, will someone else be able to see it and send an appropriate reply on your behalf? What if a password to one of your accounts is lost and someone needs to reset it by having a link sent to your email address? For reasons like these, you should give some thought to how your account itself will be handled, apart from the archived messages.

Understand Email Complexities

You've already made a list of your Email accounts in your inventory of digital assets. But before you make decisions about how your email will be handled, you should be aware of some basic facts about email that may affect how you think about it.

Where Is Your Email?

When you open your email program, you may see anywhere from a handful to hundreds of thousands of messages. And so it's tempting to think that all those messages are "in your email program," but that's almost never actually the case. In fact, your email is most likely in one of the following places:

- **In the cloud only:** If you use Gmail or any of numerous other Web-based email systems—and you check your email *exclusively* using a Web browser or a browser-based app such as Mailplane—then your messages exist only in the cloud, which is to say on the provider's servers in a data center somewhere. (If you can't see your email at all when you're not connected to the Internet, you know your messages are stored solely in the cloud.) If anyone else is to gain access to that email, they must have your username and password—but, if your account is deleted (or otherwise disabled) after you die, all your email could disappear with it unless you take extra steps to save copies of those messages elsewhere.

> **Tip:** One easy way to get a local copy of all your messages, which works with most webmail providers (including Gmail), is to set up a conventional email app to access your account via IMAP. Then (per the next bullet point) you'll have a copy of your messages on your computer in addition to the copy in the cloud.

- **In the cloud (with a local copy):** The most common arrangement is one in which your email provider stores the master copy of all your incoming, sent, and saved messages, but you *also* have a local

copy of all your messages on your computer in a conventional email app such as Apple Mail, Outlook, or Thunderbird. If you connect to your email provider with an email app as opposed to a Web browser, it's highly likely that you do so using IMAP or Exchange protocols. If so, then even if your provider is Gmail or another Web-based service, your messages normally exist in *two* places: in the cloud and on your computer. (Although it's possible to change this default behavior, few people do so.)

Even if you use an IMAP or Exchange account, it's possible to move messages out of the cloud and into local mailboxes on your device. You might do this, for example, if your email provider imposes a storage quota and you're running out of space on the server. In such cases, the messages you moved will be only on your computer, per the next bullet point.

> **Note:** Unlike email apps on desktop and laptop computers, email apps on mobile devices usually don't store copies of *all* your email messages, but rather only those in specified mailboxes, or in mailboxes you've manually opened.

- **On your computer (only):** If you use a conventional email app and you connect to your email provider using the older POP protocol, then it's most likely the case that any messages you've downloaded have been deleted from the server and exist only on your computer. (Again, it's possible to configure email clients in other ways, but most people don't.) The same may be true for any messages you received from an IMAP or Exchange account but then manually moved to a local mailbox on your computer, deleting them from the server in the process.

Note: Unsure whether you use IMAP, Exchange, or POP? Check the account settings in your email client. They'll invariably tell you which protocol the account uses. Another way to check is to file an incoming message into a mailbox on your computer, and then see if that message appears in that mailbox on another computer or mobile device. If it does, your account is set up to use IMAP or Exchange.

If messages are stored on your computer—whether or not those messages are also in the cloud—keep in mind that they aren't kept inside your email client itself. Rather, the messages are stored in a folder separate from the app—usually somewhere within your user folder (although the exact location varies from one app to the next, and some apps, such as Outlook, can store their data in any of numerous locations). I mention this because if you're backing up or archiving your data to pass on to someone else, you'll want to be sure to include your email—in fact, ideally, your entire user folder—and not just the email app itself.

I should point out that, regardless of how you access, store, or delete your email, *your* copy of a message is almost never the only one that exists. For example, you may have deleted an incoming message, but the sender probably still has a copy in their Sent mailbox. Likewise, you might delete a message from *your* Sent mailbox, but the recipient will still have a copy. (And let's not forget that you, the other party, and your respective email providers could also have one or more backup copies.) This can be good news if your heirs are trying to reconstruct an important email conversation and some of your messages are missing—or bad news if you're hoping to remove all traces of an email exchange but you can delete only your side of the conversation.

Account Access vs. Message Access

Given what I've just said about where your messages are located, if you want to provide someone else with access to your email, there are two separate matters to consider:

- **Account access:** Your digital executor will need your email account's username (usually your email address) and password to receive email sent to your address and to send email from your address. Even if you have local copies of all your messages, you should provide access to your email account to facilitate wrapping up your personal and business affairs.
- **Message access:** If your messages are stored only in the cloud (and you have no backups or archives), then account access also provides access to your messages. But because messages can disappear from servers for many reasons—and you may have multiple email accounts as well as messages that are stored only on your computer—it's important to provide your digital executor with access to your email messages themselves in the form of files on your computer or another storage device.

I cover the details of both account access and message access ahead, in Decide How Your Email Should Be Handled.

Email Message Formats

Email messages may be stored on your computer in any of numerous formats (refer back to Decide on File Formats). For example, Apple Mail uses the .emlx format, a minor variant of a common format called .eml, which can be viewed in any text editor or word processor (though you need an email app or a converter of some kind to see certain kinds of content). Outlook uses proprietary .pst files for most account types, and .ost files for cached messages from Exchange servers. Many other email apps use the .mbox database format. There

are also apps designed to archive email outside your email program; these, too, use various formats—some generic and some proprietary.

With access to your computer, your digital executor can open your email program and see all your messages, regardless of their format. But what about your descendants 50 or 100 years from now? I wouldn't assume that companies like Apple and Microsoft will still have apps that far in the future that will read today's formats. So, as a favor to future generations, I suggest that you leave instructions for your digital executor to not only preserve your email in its existing format but also export your messages in a format like plain text, HTML, or PDF that's likely to be readable a long time from now.

> **Note:** The options and steps for exporting or converting email messages vary wildly by platform and app. Ideally, your digital executor will be tech-savvy enough to figure this out. (You could do it yourself, but that will account only for the messages you've sent or received so far.) A Web search for `export email from client to format` should produce a number of helpful alternatives.

Multiple Email Accounts

Perhaps it goes without saying, but many of us have more than one email account, and they may be of different types, with their messages stored in different locations and formats. If you have more than one account, you'll need to think through the ways in which each one should be handled, and leave explicit instructions for each one.

Decide How Your Email Should Be Handled

Now that you know the major considerations and pitfalls of email, it's time to decide how you want your digital executor to handle it. You'll need to include instructions in your digital will for how each of your email accounts (refer back to the Email portion of your inventory) are managed in the short term and how your stored mail is handled.

Ongoing Email Access

In the days and weeks after your death (or during a period of illness or disability), people and companies are going to keep sending you email, just as letters, checks, and bills will continue arriving in your mailbox for a while. Your digital executor could just ignore or delete all these messages, but some of them may contain essential financial or legal information, and your correspondents will probably want to know why they're not hearing back from you. Furthermore, even the process of closing your accounts may require confirmation by email.

Although timing and circumstances will undoubtedly influence the appropriate actions when the time comes, you should think about and write down your wishes regarding at least the following:

- **Replies to real people:** If a friend, relative, or colleague sends you a message, what sort of response should they receive? Your digital executor could craft an individual reply to each person, or set up a generic automatic reply (like a vacation or out-of-office message) that goes to everyone—for example, "This is an automated reply. I'm very sorry to say that Tommy Phillips passed away on (date). Please update your records accordingly. For further information, please contact me at (phone number). Sincerely, Sara Hodges." Regardless of the approach, if you would like posthumous replies to be carried out in a certain way, be sure to say so.

- **Replies to businesses:** Companies, government agencies, charities, and other organizations with whom you've done business will need to know to close your accounts, but if you have unpaid bills or other outstanding issues, your digital executor will need to know how to deal with them.
- **Mailing lists:** Normally, the only reasonable response to a posthumous message from a mailing list is to click the Unsubscribe link. But if it's a *discussion* list on which many people participate, it may be appropriate for your digital executor to first send one final message to the list noting your passing so that other members won't wonder what happened to you.
- **Account verification and password resets:** In the course of wrapping up your estate, your digital executor may need to click links in email messages sent to your address in order to confirm account closures, recover lost or forgotten passwords, or perform similar tasks. If you have a particular email account you typically use for such administrative purposes, be sure to mention it in your digital will.
- **Account closures:** After a period of time, your digital executor should close and delete all your email accounts. If you have any reason to accelerate or delay this process for certain accounts—for example, you want a business account to be shut down as soon as possible but leave a personal account active for the benefit of correspondents you hear from only once or twice a year—make a note of your preferences.

Stored Email

For all practical purposes, I think nearly everyone will make one of only three decisions in regards to long-term access to their stored (saved and sent) email:

- **Keep everything:** Create an archive in some format that's likely to be readable a long time from now and store it safely. Don't leave it on an email server, where its long-term viability is uncertain.
- **Keep selected mailboxes:** If you're an extremely organized person and you are already in the habit of filing messages into mailboxes (or applying tags) to identify those in certain important categories, such as messages that should be passed on to a work colleague or family member, you might choose to archive only the messages in those mailboxes and have your digital executor delete the rest.
- **Delete everything:** Erase both local and cloud copies of all the messages in all your accounts.

You may wonder why I don't list a fourth option, as in "keep only specially selected messages." It's for the simple reason that *life is too short*. I don't know about you, but I have hundreds of thousands of saved messages, and even if I sorted through them at a rate of 1000 per day, it would take me the better part of a year to divide them all into "keep" and "delete" categories. It's just not worth it. It's one thing to preserve a mailbox containing messages you've specially set aside over the years, and another thing entirely to start categorizing oodles of existing messages.

That's my perspective, anyway. If you have loads of time on your hands, relatively few email messages, and a compelling need to ensure that only a subset of them survive for posterity (even though you haven't already categorized them as such), feel free to sort them and preserve just the mailbox(es) containing the messages you want to keep. But in my opinion it's lots of work for very little reward.

If you're inclined to delete everything, keep in mind my earlier statement that you can, at best, delete your own copy of each message—you can't affect the copies your correspondents have. For that reason, and because saved email can provide such a rich store of information for future generations, I suspect most people will opt to keep everything. I talk about the mechanics of doing that next.

Add Email Instructions to Your Digital Will

First, confirm that the inventory of online accounts in your digital will contains each account's username, password, and server address. (If you Use a Password Manager, all this information is likely already in it; be sure to highlight your email accounts so your digital executor can find them easily.)

> **Note:** Even if your digital executor also has access to your computer and its login password (if any) and can use it to access your accounts, it's important to include your email account details. With them, your digital executor can use another computer or mobile device to handle your accounts, which may be more convenient.

Then, under the "Email" heading in your digital will, include instructions for the following tasks discussed earlier in this chapter:

- **Handling ongoing email:** Write down any special instructions for handling replies to messages that arrive after your death (see Ongoing Email Access), including when you'd like your accounts to be closed.
- **Handling stored email:** Specify whether you want your digital executor to keep some or all of your email, or delete it all to the extent possible (refer back to Stored Email). If you have a preference as to the file format that should be used for archiving your email (for example, PDF or plain text)—or if you want your digital

executor to use a certain tool or procedure to archive your email messages—write it down here.

Warning! In order to avoid inadvertently erasing your email messages, your digital executor should not delete your account from your email app or close the account on the server until all your messages have been stored safely *outside* your email app and backed up.

Leave Posthumous Messages

Numerous services enable you to set up email, text, or video messages (or even documents) to be sent after your death. They use various schemes to ascertain when you're dead—for example, a service may ask you to set up one or more trustees in advance. If one of them contacts the service to say you've died, the service will attempt to contact you, and if you don't reply, they'll take that as confirmation. (There are many other approaches, as well, but they always include some sort of safety measure.)

That sounds useful in principle, but I'd be reluctant to count on such a service. For one thing, sites like this come and go with depressing regularity. If you set up a goodbye message but the service goes out of business before you die, your message could be lost forever. You're also counting on the technology to work correctly—but you'll never know if a posthumous message failed to be delivered for some reason, and if a message is mistakenly sent too soon, the results could be even more disastrous.

So, those huge caveats aside and purely for informational purposes, I offer a few examples of services that do this sort of thing:

- Afternote
- AfterWord
- Dead Man's Switch
- GhostMemo
- Knotify.me
- MyGoodbyeMessage
- remember-me
- To Loved Ones

Deal with Social Media

Your social media accounts, such as Facebook and Twitter, can live on (in a sense)—if you want them to.

Do you use Facebook, Twitter, LinkedIn, or other social media services? (If not, nothing to see here—skip ahead to the next chapter, Deal with Other Digital Data.) You may want a loved one to post a

final message on your behalf, or you may want to hand ownership of the account to someone else. You may also want to have your messages archived (online or offline).

As is the case with email (see Deal with Email), there are also some people who shudder at the very thought of their social media accounts existing at all after they've died, and would prefer for the accounts to be shut down and expunged from the cloud.

Regardless of how you approach social media, it's worth reviewing what you have, how you use it, and what your options are for the future—and then to include those wishes in your digital will.

Review Your Social Media Accounts

Earlier, in Social Media, I asked you to create a list of your social media accounts (such as Facebook and Twitter) to include as part of your inventory of digital assets. Refer back to that list now.

Take a few minutes to log in to each of the accounts on your list and skim through your posts, photos, and other information. For each service on your list, make a few notes about the extent to which you use it and how important it is to preserve its data. You can then choose any of several approaches for dealing with each account, as I describe next.

> **Note:** Even if you authorized a social media service to preserve your data in perpetuity, the law may in some cases permit your executor or other legal representative to request its deletion. Therefore, be sure to state your wishes clearly in your digital will and talk them over with your digital executor.

Decide What to Do with Each Account

On a new page of your digital will, under the heading "Social Media," list each of your social media accounts along with their respective usernames and passwords, and how you'd like your digital executor to handle them.

> **Note:** If you Use a Password Manager, it should already contain the usernames and passwords for your social media accounts, so you can omit them from this list—but you'll still want to list your wishes for how each account will be handled.

Although not every service offers every option, your choices usually include the following:

- **Final words:** Your digital executor can post a final farewell, so that anyone who sees your account in the future will know what happened and why you aren't posting anymore. If you have a specific message you'd like to include, write it down.
- **Archive (online):** Some services let you memorialize the account of a deceased user in such a way that they remain online indefinitely (for example, as a place for loved ones to post memories and condolences) but limit or disallow most access.

> **Tip:** Facebook gives you the option to set up a legacy contact—someone you authorize in advance to memorialize your account (including posting a final message) or delete it when you're gone.

- **Archive (offline):** Most services give you the option to download all your posts so that you can store them locally and pass them on, whether or not the data also remains online.
- **Delete:** A deceased user's account can be deleted completely, making its posts inaccessible to the public in the future. (If you do this, I suggest archiving the site's data offline first.)

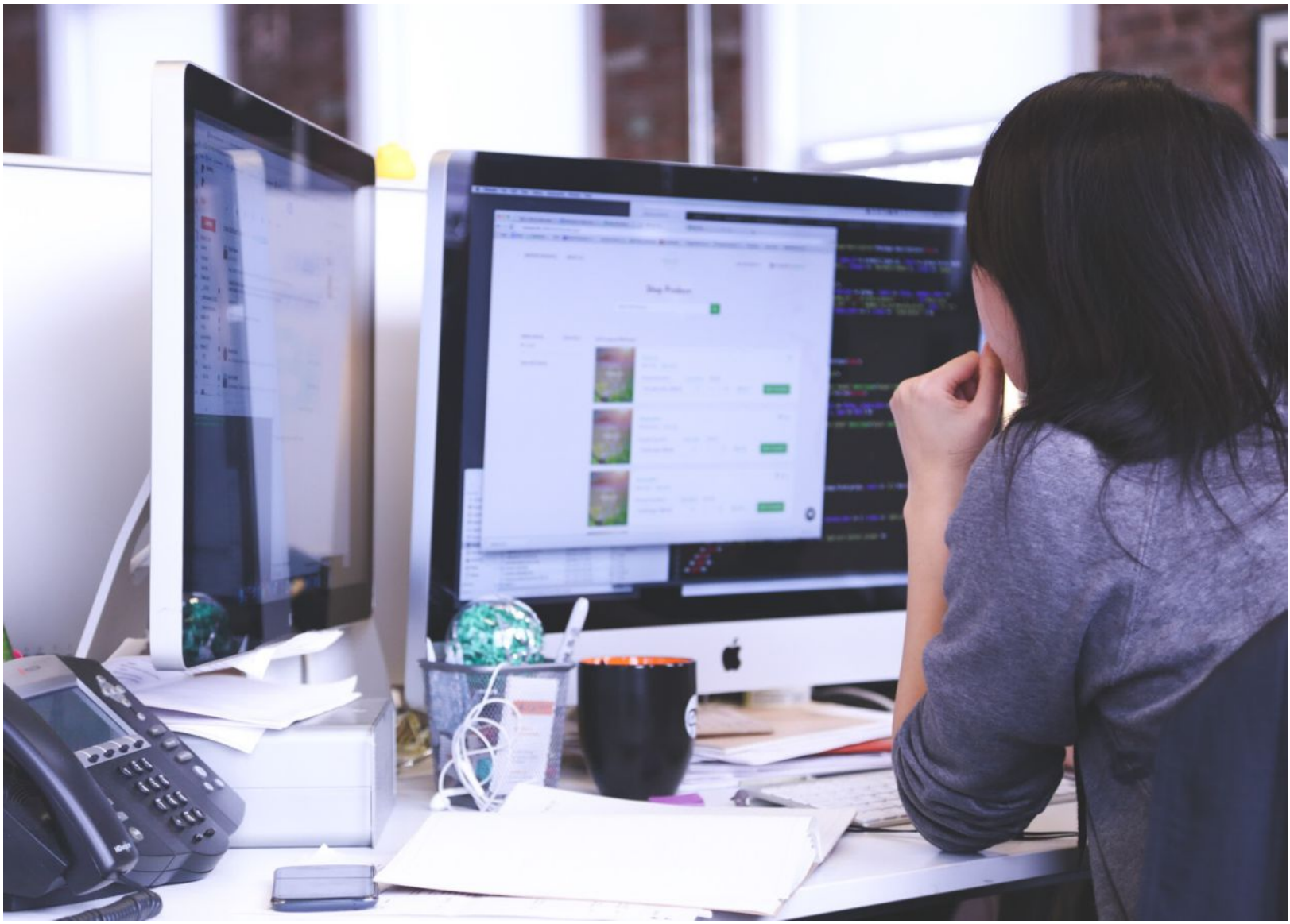
- **Hand off:** In some situations, you may want to pass access to your account on to a friend or loved one. For example, if you have a Twitter account you used for sharing tips or suggestions on a favorite topic, your followers might appreciate it if someone else took over to deliver similar information.

> **Note:** Some sites either discourage or expressly disallow handing off *personal* accounts. For example, it would be problematic at best to let someone else use your personal Facebook account after you die, but if you have a fan page or administer an account for an organization, it's generally appropriate for someone else to take it over.

Each site has a different procedure for archiving or deleting the account of a deceased user. In most cases, your digital executor will need to provide a death certificate and several other pieces of information. You (or your digital executor) can consult the following pages for details:

- Facebook: Special Request for Deceased Person's Account
- Google (including Google+ and YouTube): Submit a request regarding a deceased user's account
- Instagram: How do I report a deceased person's account on Instagram?
- LinkedIn: Deceased LinkedIn Member - Removing Profile
- Pinterest: Reactivate or deactivate an account
- Tumblr: How To Close A Tumblr Account When Someone Dies
- Twitter: Contacting Twitter about a deceased or incapacitated user
- Yahoo (including Flickr): Options available when a Yahoo Account owner passes away

Deal with Other Digital Data



Your media, software, and other miscellaneous digital data needs to have a plan, too.

The previous several chapters detailed how to deal with major categories of digital data, such as photos, accounts, email, and social media. This chapter is about everything else—all the other bits (see Inventory Your Digital Assets) for which you should record your wishes.

Although these topics aren't long or complex, they're no less crucial than those I covered earlier. For example, they include all the miscellaneous files and software on your computer, as well as data you've stored in cloud services such as Google Docs and Dropbox. This chapter also covers how to handle backups and archives of your data, whether you've stored them on hard drives or optical discs, in the cloud, or in some other way.

Handle Your Media

In Inventory Your Media, I asked you to list your audio and video media and ebooks, divided into that which you've purchased and that which you obtained in other ways.

Media you *didn't* purchase (and that, presumably, has no DRM protections) can be distributed in almost any way you choose; simply record your wishes in your digital will. Keep in mind, however, that unless you created it yourself, even DRM-free media is subject to copyright laws, and therefore should not be passed on to more than one person.

But, as I explained in An Aside: Digital Media Complications, leaving purchased media to anyone is potentially problematic:

- Unlike photographs and other digital documents that can be copied and passed on to multiple people, DRM-protected media can, at best, be passed on to one person.
- To play media protected by DRM, the other person will need your account credentials, which may prove inconvenient; and even then, there are various circumstances under which the provider could cut off access to the media.
- Although DRM is less often applied to purchased music than to video, the practice varies by provider.

- Any media you pay to stream (such as Netflix videos or Apple Music) will stop being available when your account is closed, so you shouldn't consider it an asset at all.
- Although a relative or friend might appreciate having access to your purchased media, it won't have the same sort of sentimental or historical value as your other data, because it's not unique—anyone can purchase the same media you did.

For these reasons, whatever choices you make regarding your purchased media, you should do so recognizing that it may be beyond the technological capabilities or legal authority of your digital executor and beneficiaries to carry out your wishes precisely. That said, your major options are as follows:

- **Destroy it.** If you don't want anyone to have to deal with the potential ramifications of copyright and DRM, you could write off all that media and ask your digital executor to erase the files.
- **Leave it all to one person.** If a particular beneficiary seems to be a good recipient of your purchased media, state that person's name and exactly what items you want them to have. Your digital executor will need to figure out how to transfer the necessary files (on an external hard drive, for example). Be sure to include in this portion of your digital will the username(s) and password(s) applicable to the account(s) where the media was purchased, and mention any software that may be needed to play the files.

> **Note:** If you do choose to leave your media to someone, you should explicitly *exclude* it from the archives you create with the rest of your data (as discussed in the next chapter, Preserve Your Data for Posterity), because those media files won't be useful to anyone else.

- **Pass the buck.** If you're unable to decide what to do, or if you can't be bothered to think through all the complexities involved, you can ask your digital executor to make decisions about your purchased

media on your behalf. Between now and then, changes in technology or the law may affect the ways in which your media can be handled, and if your digital executor is willing to take on the responsibility of figuring it out, this is not a terrible choice!

Handle Your Software

As I noted in Inventory Software, your digital will should list the apps that will be needed to open your important files (to facilitate the process of archiving your data, if applicable), those that require subscriptions (so they can be cancelled), and those you would like to bequeath to someone else. Because the first two categories are self-explanatory, the only thing you should need to add to your digital will is who is to be the recipient of any software you intend to pass on.

Handle Digital Currency

If you own any bitcoins or other digital currency (see Inventory Digital Currency), remember that this is *actual money*—as valuable as dollars, euros, or yen, just in a different form. You can leave it to anyone you like, as long as your digital will specifies in detail how to access the money. But note that, as a tangible asset, it will be subject to taxes, and that either you or your digital executor will need to discuss the details with the executor of your conventional will.

Handle Other Cloud Data

Among the accounts you noted earlier (in Inventory Online Accounts and Highlight Key Accounts) are some containing data that doesn't also appear on your computer or elsewhere in your digital archive. In addition, some of these accounts may do more than just hold data; they may make that data available to other people, for instance.

In any case, you'll need to state in your digital will, for each account, both what should happen to the online data and what should happen to the account itself.

Your choices for the online data include:

- Download it and add it to your digital archive.
- Erase it from the cloud.
- Transfer the files to someone else.

And, for the accounts themselves, your options include:

- Shut down the account.
- Have your digital executor keep it going for a while.
- Transfer ownership of the account to someone else.

Since these options may sound a bit abstract, let me give you a few concrete examples:

- **Dropbox:** In most cases, the files in your Dropbox account are also synced to your computer, so they'll appear in your digital archives without further effort. However, if you've shared certain folders with other people and your digital executor shuts down your entire account, those other people may lose access to the shared files. If that could pose problems, spell out your wishes—for example, have your digital executor inform a specified list of people that they must make copies of any shared files they want to keep within 30 days, after which the account will be deleted.

> **Note:** Dropbox is, of course, just an example; the same applies to any service used to store or sync files in the cloud.

- **Your Web site(s) and domain(s):** If you have your own Web site (or more than one!), the HTML documents, images, and supporting files should probably be downloaded and added to your digital

archive in case someone wants to see them in the future. But if the site is to remain online, someone else must be given the credentials to access it (and must take over paying for the Web hosting account, too). If you own domain names, the same applies to them; and, if you purchased them from a registrar other than your Web host, you should include the registrar's name and instructions for how you want the domain names to be handled.

- **Your medical records:** If your health provider offers online access to your medical records, you may want to request that your digital executor download all the files and then instruct the provider to close your account.

> **Note:** Online backups also count as "other cloud data," but I've addressed them separately ahead, in Handle Backups.

- **Instant messaging histories:** Some instant messaging services, such as Apple's iMessage, store histories of your conversations online. Those histories are most likely synced to your computer as well (and indeed, sometimes they're accessible only in an app on a computer or mobile device, not in a Web browser). But if you have any accounts with services that store instant messages online—and you want to preserve those messages—be sure to note your wishes.

- **Ebooks that use DRM:** Most ebooks sold by Amazon, Apple's iBooks Store, and similar vendors use DRM. Even if you've downloaded the books and stored them in an app, on a Kindle reader, or on another device, it's both technically and legally iffy that you'll be able to transfer them to someone else. In other words, ebooks protected by DRM are much like downloaded videos, and all the same caveats apply (refer back to Handle Your Media).

> **Note:** Some vendors, including Amazon, permit publishers to choose whether or not to apply DRM to their books. Take Control opts not to use DRM, for example.

On the other hand, ebooks you download in PDF format (including this one—if you aren't reading this ebook in PDF format, see Ebook Extras to learn how to download a PDF version) aren't copy protected and can be transferred just like any other file, as I discuss in the next topic.

Note: PDF documents can be password-protected, although that's different from copy protection (and I've never heard of a password-protected commercial ebook). I say more about encrypted and password-protected documents ahead, in the sidebar Encryption and Password Protection.

Handle Other Local Data

Earlier, in Inventory Other Personal Data, I asked you to create a list of the major types of miscellaneous files on your computer and where to find them. Of the items on that list, you already should have recorded your wishes for email (in Deal with Email) and your audio and video media (in Handle Your Media). Now you need to specify what to do with your other files—including your photo library.

If, like me, you have hundreds of thousands of personal files on your computer, the whole notion of going through your inventory—even by broad categories—and specifying your wishes individually is probably both daunting and pointless.

So, in the interest of keeping things simple, I suggest that you assume *all* your photos and miscellaneous files will be kept and passed on to your heirs (the mechanics of which I cover in the next chapter, Preserve Your Data for Posterity), and simply make a list of any items or categories that you want your digital executor to delete, omit from your archive, or distribute to certain people. For example:

- **Academic or professional research:** If you have files representing work you did for school or business that may prove useful to a

colleague, a university, or some other entity, specify which ones those are and how they're to be distributed.

- **Personal memorabilia:** Perhaps your computer contains letters, photos, historical documents, genealogical data, or other personal bits that certain family members would especially appreciate seeing. Be sure to specify what goes to whom. On the other hand, if you have love letters to or from someone your spouse would just as soon forget—or other documents that you consider embarrassing or sensitive, you may ask your digital executor to omit them from your archive and delete the originals.

- **DRM-free ebooks:** If you have any ebooks in PDF format (or otherwise lacking copy protection) that you want to leave to a particular person, make a note of them.

- **Other people's archives:** As I mentioned in the sidebar Including Someone Else's Digital Legacy in Yours, if someone else has entrusted you with their digital legacy, all that person's digital files should be subsumed into your own archive, so that they'll be preserved and passed on properly. But you should still call attention to those files so your executor knows what you have and whether anyone else in particular will need access to it.

As I say, these are merely examples, but my point is that you shouldn't devote days of your life to spelling out your wishes. Just hit the highlights of anything to which you want to give special treatment.

Encryption and Password Protection

If your data includes any files that are individually encrypted or password-protected, such as confidential PDF documents, data used by financial apps, or (on a Mac) encrypted disk images, be sure your digital executor has the necessary passwords to open them. You can store these in your password manager or list them separately.

Handle Backups

I hope you've been religiously backing up your computer for years, and that you'll continue doing so as long as you're alive. (If not, see my recommendations in Back Up Digitized Files, which apply to everything on your computer—not just files you've recently scanned.) The question is what should happen to those backups once you're gone.

In the next chapter, you (or your digital executor, or both) will be transferring the majority of data from your computer to archival media. And, in theory, that should be that; after you're dead, those archives should take over the function that backups currently serve. However, because I've seen enough things go wrong with computers and backups I believe that an *extra* backup never hurts.

My suggestion is that, in your digital will, you instruct your digital executor to do the following:

- Turn off your backup software so there's no risk that it will accidentally overwrite or delete files already in your backups.
- For backups stored locally (for example, on external hard drives), disconnect the media and store it in a safe place—at least until the final archives have been created, copied, and verified.
- If you use an online backup service, such as Backblaze or CrashPlan, keep the service active until the archives are complete. If online backups are your *only* backup, and the service you use offers the option to have your backups returned on a hard disk or flash drive (as Backblaze does), do that.

Preserve Your Data for Posterity

What you're creating amounts to a time capsule that will need to be preserved so people far in the future can see and appreciate your data.

You've catalogued your digital data and decided what should be done with it when you're gone. That's terrific—and essential—but if your plan hinges on a great-grandchild being able to boot your old iMac that's been passed down for generations, you've still got a problem.

Imagine finding a 1981 IBM PC, forgotten for decades in an attic. It might still turn on, or maybe not. Depending on the configuration, it may have included a hard drive or, more likely, 5¼-inch floppy drives or even a cassette drive for data storage. Let's be optimistic and say the media was stored with the computer. Will it still be readable today even if the computer works? Perhaps, but I wouldn't count on it. And if you're lucky enough to be able to see those old files on a screen, you still have the challenge of getting the information onto a modern computer (or even printing it).

That's what today's devices will look like to your grandchildren. And even if you store them in museum-like conditions, machines, media, and the data they contain deteriorate over time. You can't control how technology will change years in the future, but you can take steps to increase the likelihood that future generations will be able to read the files you've so carefully preserved. The first part of this chapter covers which media to use, how to preserve it for the near future, and instructions you can leave that will help your data last into the more distant future.

In addition, even if your current devices won't be passed on for generations, they could be incredibly valuable to the person handling your estate, so you should also Decide What to Do with Your Hardware.

> **Tip:** Since your digital executor will be intimately involved with handling your data, I recommend discussing your choices here (media, file formats, and so on) with them and involving them in the decisions.

Choose Archival Media

In museums and libraries, you can often find books that are hundreds of years old, and other documents (scrolls, papyrus, clay tablets, and so on) that are much older. But for every document that survived hundreds or thousands of years, a vast number of others did not. All

the conditions have to be just right, because heat, humidity, pests, mold, and other environmental factors can destroy almost anything over a long enough period of time, and organic substances like paper are especially vulnerable.

Even so, much of today's digital media is, if anything, far *more* susceptible to the ravages of time than old-fashioned paper. The magnetic particles that store data on the platter of a hard drive can lose their charge over time, even if the disk hasn't been used. And, although the storage mechanisms (and the ways in which degradation occurs) vary, almost all other modern media can also lose data over a period of years or decades—that includes CD-ROMs and DVDs, digital tape, and flash memory. On the other hand, what's great about digital media is that it's so much easier to copy, over and over, than paper and other, older forms of media.

So, what are your options? Well, there is currently no *ideal* long-term option, but let me walk you through the pros and cons of a few alternatives you might consider. Any of these should be good for at least 10 years, but see Refresh Your Archives for advice about longer-term maintenance.

Archival Quality Optical Discs

A number of companies make recordable CDs and DVDs—usually using some type of gold and/or silver formula—that will supposedly preserve their data for a century or more. For example:

- Media Supply sells JVC/Taiyo Yuden archival discs, such as DVD-R, with an estimated 100+ year life.
- Delkin Devices sells archival gold storage media, including CD-R with an estimated lifespan of 300+ years, DVD-R estimated at 100+ years, and Blu-ray estimated at 200+ years.

- M-Disc media are supposed to last for 1,000 years, and come in various formats including DVD and 25, 50, and 100 GB Blu-ray.

There are, however, two potential problems with archival optical discs:

- **Longevity claims can't be verified:** How do you *know* the discs will retain their data for the centuries their manufacturers claim? The passage of many decades could have unseen effects that today's engineers couldn't foresee. By the time someone figures out that there's a problem, the company that made the discs will have long been out of business.
- **Compatible equipment won't last:** Supposing a DVD is still perfectly readable 100 years from now, where are you going to find a DVD drive that still works, and that can connect to the computing equipment of the far future? Even today, it's increasingly rare to see new computers come with optical drives, which were once standard equipment. If you think about how hard it is to read a floppy disk on today's computers, and then multiply that difficulty by a factor of 10 or so, you'll have a pretty good idea of what that archival media might look like in a few generations.

Although these problems are not insuperable (especially if your heirs transfer your archive onto new media every so often; see Refresh Your Archives), they certainly make optical discs less than a slam dunk.

Hard Drives or SSDs

External hard drives may seem like a logical choice, because they're inexpensive, ubiquitous, capacious, and fast. But are they reliable enough to use for long-term storage?

To the best of my knowledge, the longest warranty offered today on any consumer-grade hard drive is 7 years, and most are much shorter. Of course, a warranty simply means the company will replace a drive

if found to be defective during that time, not that your data is guaranteed to remain intact! And I've had so many hard drives fail after only 3 or 4 years that I can't imagine trusting any hard drive—warranty or not—for 10 years, let alone centuries.

A hard drive that sits idle for years is less likely to develop mechanical failures than one in constant use (although plugging it in occasionally, just to let the drive spin up to speed, can prevent the mechanism from getting stuck). But even careful preservation of a drive can't prevent magnetic charges from dissipating over time, leading to data loss.

SSDs are also subject to eventual, random data loss, but because they have no moving parts and don't rely on magnetic charges, they tend to preserve data longer than hard drives—at least if the SSDs are not used. Indeed, I've heard of at least two SSD manufacturers (SanDisk and Patriot) that offer 10-year warranties on some models. So, I'd have greater confidence in SSDs for semi-long-term storage, but my enthusiasm is offset by their considerably higher prices.

So, if you are considering a hard drive or SSD for archival storage, observe these tips:

- Not only should you get more than one drive (see Store Media Safely (and Redundantly), ahead), but you should also get different brands.
- If financially feasible, use an SSD for one of your copies.
- All things being equal, prefer brands and models with longer warranties.

Cloud Storage

Another option is to commit your long-term archives to the cloud. Although cloud storage uses conventional technologies such as hard drives and SSDs, nearly all providers have their own backups, as well as mechanisms to correct errors and programs to refresh the hardware

as needed. And some cloud storage is even free (for a limited amount of data). So it's certainly tempting to commit a few gigabytes of files to, say, Amazon Cloud Drive, Dropbox, iCloud, or Google Drive (among many other choices) and just assume it will be there forever.

Unfortunately, you have no way to know that even today's biggest companies will still be around decades from now; that they'll still be offering cloud storage then; and that nothing will go wrong on their servers that might endanger your data. Furthermore, if your cloud storage is tied to your personal account, and that account is closed after your death (intentionally, or automatically due to an extended period of inactivity), all your data will disappear. Plus, if you need more storage than you can get for free, someone will have to keep paying those monthly or annual bills in perpetuity!

In response to problems like this, a service called Chronicle of Life claims to provide *permanent* cloud storage for a modest one-time fee. The site tells a great story about how the service is funded and the terrific ideas driving its ambitious guarantees. And yet, I couldn't help noticing at the beginning of 2017 that the copyright date on the bottom of every page still reads "2008–2015," which doesn't inspire confidence.

A similar service, called Forever (which also offers photo scanning and storage of physical materials) has a slightly less ambitious guarantee: they'll store your stuff for your lifetime plus 100 years. But Forever has been around only since 2013, and it's difficult to judge how robust its plans are. Because I've seen so many other digital legacy services go out of business, I'm reluctant to trust these, no matter how appealing their marketing copy is. At the very least, if I chose a service like this, I would hedge my bets with a secondary means of storage.

However, there's another option you might consider, *if* you're comfortable making all your data public after your death: uploading it to The Internet Archive. This massive, nonprofit digital archive contains

vast amounts of archived material—Web sites, movies, audio, photographs, documents, and much more. You can create a free account that permits you to upload your own materials (items that are in the public domain or for which you hold the copyright), which then become a permanent part of the publicly searchable archive. See the FAQ for more information on licensing, filenames, formats, and other issues. (Also see the sidebar Donating Documents to a Public Archive, ahead.)

Paper

I know it's old-fashioned, but given the state of today's technology, paper—carefully stored—may still have a longer shelf life than most other media. Obviously, you won't want to print out tens of thousands of pages of documents, and paper won't help you with audio or video files. But you should certainly consider printing and preserving paper copies of your most crucial documents, within reason.

Sapphire

A company called Fahrenheit 2451 claims to have the ultimate in long-term storage—something that's not subject to any of the problems I've listed with other media. It sells custom, laser-engraved sapphire disks called *nanoforms*, 2 or 4 inches in diameter, which can each hold up to 2,500 documents or photos. The company says the nanoform is fireproof, waterproof, and impervious to magnetic fields and even *lava*. As long as you don't lose the disc or destroy it in an explosion, it should be viable millennia from now.

Interestingly, the laser engraving process doesn't store ones and zeroes on the disk; rather, it's like an extremely high-resolution, monochrome printout. So how do you retrieve your stored information? With a microscope or a strong magnifying glass, of course! That neatly solves the problem of compatibility with future devices, although it also limits the types of data you can store—no audio or

video, for example, and although color photos can be stored as separate red, green, and blue images that a computer can later recombine, that's not an approach you'd want to take with more than a handful of pictures.

How much does eternal storage in sapphire cost? Well, the 4-inch nanoform runs €1,130 (about $1,200), while the 2-inch version costs €520 (about $550). And you thought SSDs were expensive!

So, I mention this more as a novelty than a serious suggestion, but also to point out that every option has at least one trade-off. You can solve any given problem only by creating one or two more!

Donating Documents to a Public Archive

Earlier, I mentioned the possibility of uploading documents to The Internet Archive as a way of both preserving and publicizing them. Whether or not you do that, you may want to consider donating documents to a public archive, historical society, library, or other institution. Your donated data will then become available to the public, including historians, academics, and other researchers. And because you'll be putting your materials in the hands of trained archivists, the odds that they'll be preserved properly go way up—and neither you nor your heirs will have to worry about storing data or refreshing it (as discussed later in this chapter).

Generally speaking, public archives are interested only in documents they consider to have historical significance. You'll have to talk to an archivist to determine whether any or all of your data may be of interest to them—and, if so, how to organize and deliver it. For further details and advice, read Donating Your Personal or Family Records to a Repository at the Society of American Archivists.

Create a Data Archive

Once you've chosen the media you want to use (or, perhaps, you've decided to hedge your bets and use two different media), it's time to copy your data from your computer onto the archival media.

There's no special trick or magic to this—copying data is pretty much as boring and anticlimactic as it sounds. However, I'd still like to make a few recommendations, which hold regardless of the type of media you're using:

- **Err on the side of inclusion:** Because we're only copying data here, not your operating system, there's no need to include the various folders that make up macOS or Windows. Most people store all user-generated files somewhere in their home folder, which means you can usually copy just that folder and not give the process much more thought. *However*, if you know you've stored some files elsewhere, be sure to copy those too. And, when in doubt, it's much better to copy more files—even ones you're pretty sure no one in the future will ever need—than to leave out files that might be useful.

> **Tip:** If you're a Mac user who stores files in iCloud Drive, I suggest copying the contents of your iCloud Drive folder separately. Select iCloud Drive in the sidebar of a Finder window, select all the folder's contents, and drag them to your destination media.

That said, as I mentioned in Handle Your Media, if you're planning to leave purchased media (such as movies and TV shows) to someone else, you should exclude those files from your archive, and instruct your digital executor to copy them from your computer to suitable external storage when the time comes. There's no point in including massive amounts of video data in an archive, if that portion of your data will be usable by, at most, one person.

> **Note:** If you are preserving someone else's digital legacy as part of your own (see the sidebar Including Someone Else's Digital Legacy in Yours) and those files aren't already on your computer, be sure to copy them to your archival media now.

- **Use a backup app:** Depending on your operating system and the media you've chosen, you might be able to use drag-and-drop or copy-and-paste to copy data from your computer onto the archival media, and in general, those approaches are fine. However, you might instead consider using a backup app, which might be simpler, and which is more likely to verify that all your data copied correctly.

  If you do use a backup app, however, be sure you use one that stores your data in a format that can be read in the Finder (macOS) or Windows Explorer, as opposed to a custom archive format. You want to be sure that no matter what device is used to access this data in the future, it will be readable without any special software.

> **Tip:** On a Mac, an app like Carbon Copy Cloner or ChronoSync would be my top pick for this task. Just be sure to tell it to copy only the folder(s) you need, not the entire disk.

- **Export as an extra step:** Back in Decide on File Formats, I suggested that—depending on what kinds of data you have, what formats it currently uses, and how much time you have—you might want to consider exporting certain kinds of data in more future-friendly formats. For example, you might want to save a copy of your saved email in .mbox format, or all your letters as PDFs; or you may want to export all the photos from your photo library as independent TIFF images.

  If you choose to export some of your data, I suggest *first* copying the data in its existing, native format, and then exporting it, in its new format, to your archival media. But *keep both copies*. That way, if someone discovers years from now that an error occurred with one of the exports, the original files will still be available for another attempt.

Now that you have a data archive, *make another*. Yes, I'm suggesting that you to go through the process of copying your data to other media at least twice, and more than twice is even better. Because any one disc, drive, cloud service, or whatever can go kaput for any of countless reasons—and this *is* your legacy we're talking about here—I recommend making at least two copies of everything. And, in my experience, you're likely to get more reliable results when making extra copies directly from the originals than making copies of copies.

In my opinion, it's ideal to have at least one local copy (on physical media you can control) and one copy in cloud storage of some kind. Despite the potential drawbacks of cloud storage I mentioned earlier, the fact that your data will be sitting on professionally maintained servers (which will be backed up and receive regular hardware upgrades) should go a long way toward keeping it safe.

In addition, thinking back to the sidebar Including Someone Else's Digital Legacy in Yours, if your digital executor (or another family member) can incorporate your data into their live data—continually backing it up and preserving it along with their day-to-day files—its chances of persisting into the distant future (and of being useful to that person) go way up!

Store Media Safely (and Redundantly)

Once you've gone through all the trouble of archiving your incredibly valuable data—twice!—you'll want to be sure that media won't be lost, stolen, or damaged in the coming years.

Here are my recommendations for storage of the local copy or copies of your data archive:

- **Choose a cool, dry, dark location.** Heat and dampness can damage almost anything. Optical discs are also especially vulnerable to light, but since light and heat often go together, I suggest a dark location for any type of media.

- **Protect against physical damage:** In your home, a safe—especially one that's rated fireproof for media—will protect your archive from fire, theft, earthquake, wind, and most other threats. As a bonus, the safe will act as a Faraday cage, protecting hard drives and SSDs from damage by electromagnetic pulses. A safe deposit box at a bank has the same advantages.
- **Store multiple copies separately:** If you have two copies of your data archive, store them in two separate locations—for example, one in a safe in your home and the other in a safe deposit box. If your archives are stored together, any disaster that wipes out one of them will wipe out the other too.

> **Tip:** For advice on safes, see The Best Fireproof Document Safe at The Wirecutter.

Refresh Your Archives

Once your data archive is safely stored, you can breathe a sigh of relief. But I hope you'll continue breathing for many years to come! And as long as you do, you'll continue accumulating new data. So you'll probably want to refresh your archive from time to time by repeating the process of copying (and, perhaps, exporting) data to archival media. Archival optical discs (and sapphire discs) can't be erased and rewritten, so you'll have to start over with fresh media; with hard drives, SSDs, and cloud storage, you can overwrite or add to your archive at any time.

How often you choose to do this is up to you, but I would suggest at least every 3–5 years for the rest of your life. If you create quite a bit of data, perhaps an annual refresh would make more sense.

In addition, you should include, in your digital will, instructions for your digital executor to update your archive, one last time, immediately after your death. That way, the archive's final form will also be

its most current; but if your computer should be lost, stolen, broken, or otherwise inaccessible when the time comes, at least your digital executor can fall back on the most recent update you made to your digital archive.

A moment ago I referred to your archive's "final form," but that was in fact premature. Unless or until technology presents us with a way to be sure our data will be readable indefinitely, your digital executor and your heirs will need to perform periodic updates of your archive for decades to come, in order to guard against data degradation. Of course, you can't guarantee that this will occur, but you can at least include, in your digital will, a reminder that you want it to occur, with a stern warning about the consequences if it doesn't (namely, the eventual disappearance of important portions of your data).

My advice for long-term archive maintenance is as follows:

- **Update archives at least every 10 years.** I don't trust current media to be readable longer than that, no matter what the warranty or marketing claim is.
- **Verify the data.** The first step in maintenance is to make sure your files are still readable (by opening a random selection of them). If they aren't, the person doing the maintenance should try your secondary copy. You don't want data errors to be propagated in future versions of your archive.
- **Copy onto fresh media.** Your digital executor or heir should obtain new media—whatever, at that point in time, seems most likely to be useful many years in the future—and make a fresh copy of your archive.
- **Redundancy is still important.** Ideally, the person maintaining your archive every 10 years or less will make at least two copies of the data, preferably on different types of media, and store them in different locations.

Decide What to Do with Your Hardware

Because your data archive is stored separately from your computer, you can be fairly flexible when deciding on the disposition of your computer, mobile devices, external storage, and so on. All those items should be listed in your *regular* will, since they are ordinary, tangible possessions.

However, I do want to make one suggestion. Your digital executor will need at least temporary access to your computer and other devices, in order to create one last update of your digital archive (and perform certain other tasks you may have assigned, such as deleting certain files or accessing your password vault). Therefore, it might be most convenient to make your digital executor the beneficiary of that hardware; but if it's ultimately destined for someone else, be sure to spell out the need for temporary access in your will.

Create a Legacy Dossier

It's time to wrap up all the documents you've created into a (paper and/or digital) dossier.

Early in this book I advised you to Begin Drafting Your Digital Will, and I hope you've been adding to it and refining it as you've gone along. And, in the previous chapter, I explained how to Preserve Your Data for Posterity by choosing appropriate media and storing it carefully. Your digital will, and your data itself, are obviously key components of your digital legacy.

However, in this final chapter I'd like to go a step further and urge you to create a legacy dossier for yourself. This will be a collection of documents (which, ideally, should exist in both physical and digital forms—for example, printouts in a folder plus a flash drive containing digital copies) that includes your conventional will, your digital will, and several other pieces of information that collectively constitute the information about yourself that you want to pass on:

- **Instructions:** An overview of what's in the dossier, how to use it, and a summary of your wishes and concerns
- **How to be me:** An explanation of how to do key business and household tasks that will help your executor—and may also come in handy as a reference for yourself
- **Your autobituary:** Your self-written obituary, in which you get to portray yourself exactly as you want to be remembered
- **Genealogical and biographical data:** Curated facts about yourself, your family, and your ancestors

You'll put this in a safe and accessible place for your next of kin or digital executor, and update it from time to time as needed.

Instructions

Speaking as someone who has had to puzzle through the assembly of way too many toys and pieces of furniture that included lots of pieces but lacked adequate instructions, I would like to urge you to include, as the very first thing a person will find when opening your dossier, a simple "Read Me" file explaining what this collection of documents is and what to do with it.

This instruction page should be quite brief, and it should basically provide a table of contents for the dossier along with a one- or two-sentence summary of how each component should be used.

How to Be Me

Throughout this book I've mentioned cases in which portions of your digital legacy may be useful to someone else while you're still alive—but on vacation, ill, or otherwise unable to discharge your usual obligations. Although your digital will provides access to your passwords and instructions for closing or carrying on various accounts, one component it doesn't include is how someone else can do the day-to-day personal and business tasks that, at present, only you know how to do. This sort of information is as valuable to a house-sitter or a spouse taking over during a hospital stay as it is to your digital executor.

I propose that you address this need by writing a brief instruction manual of sorts that explains how to be you. As a bonus, this document may help you remember how to do a few things you do infrequently.

If I had to document how someone else were to go about doing everything I do during a given day—using every app, making every decision, processing every email message—I'd be writing instructions for the rest of my (hopefully quite long) life. For the purpose of your legacy dossier, I'm not talking about anything nearly so detailed. When I say "brief," I mean it!

Because every person, household, and job is different, I can't tell you exactly what your mini instruction manual should include, but let me offer some suggestions and examples:

- **Essential tasks that aren't on your calendar.** Maybe you alone know that on the 15th of every month, your gardener must be paid in cash; or that every March you need to clean the gutters before the spring rains hit; or that you have to leave your garage door unlocked every Saturday morning so your neighbor can borrow your lawnmower. If someone handling your affairs temporarily

or permanently would never be prompted (for example, by receiving a bill in the mail or seeing an appointment on your calendar), make a note of the tasks that have to be done and when they must occur.

- **Technical tasks.** Perhaps someone taking over from you would need to know how to reboot your Web server, Wi-Fi router, or other essential device if it starts acting up; prevent a finicky alarm system from going off at the wrong time; or perform some other minor technical task for which reading an instruction manual may not be sufficient (if the other person can even find the instruction manual).
- **Financial tasks.** If a person or company needs to be paid, a tax statement filed, or another financial task performed at a specific time in order to prevent dire consequences, you'll need to explain what those tasks are and how someone who isn't you can accomplish them.

In other words, what you're trying to record is not a complete, step-by-step instruction manual for someone to take over your work or life, but rather a few pages of helpful hints that document things that are currently only in your brain. These instructions will enable someone to keep up with your major business and personal obligations—things without which you or your family would suffer serious consequences.

A Copy of Your Will

The original copy of your will is probably stored in a safe deposit box, on file with your lawyer, or in another safe place—as it should be. However, as one of the recurring themes in this book is redundancy, I'd like to suggest that it can't hurt, and will very likely help, to have an additional copy of your will stored in your legacy dossier.

Your Digital Will

Throughout this book, you've been creating and adding to your digital will. This document should now have a complete, detailed record of your instructions for your digital executor, including how to access all your key accounts, what types of documents you've stored and where, and how you want all your digital assets to be disposed of. That document is perhaps the most important part of your legacy dossier.

Assigning Legal Authority to Your Digital Executor

I am not a legal expert—and in any case, laws vary from one jurisdiction to the next—but there could certainly be situations in which your digital executor needs legal authority to manage certain accounts on your behalf after your death. The mere existence of an informal document like a digital will may not necessarily be sufficient to convey this authority.

A lawyer can tell you whether, or to what extent, the authority of the digital executor should be spelled out in your conventional will—and whether additional steps, such as assigning this person power of attorney, should be taken before your death.

Your Data (or Where to Find It)

Remember that data archive you created in the previous chapter, Preserve Your Data for Posterity? If it's stored in a form (say, a recordable DVD) that can easily go in the physical folder in which you keep your legacy dossier, put it there. If it's either too large (an external hard drive) or not a physical object at all (cloud storage of your data), at least include a page that provides detailed instructions about how to find it.

Your Autobituary

You know the old saying: if you want something done right, do it yourself. I wish I could take credit for coining the term *autobituary,* but it has been circulating for a while. It's nothing more or less than an obituary written (before death, obviously) by the person it describes.

I've seen a number of these; one, which achieved a period of viral fame in 2014, was for Walter G. Bruhl, Jr., of Newark, Delaware. Walter not only laid out the salient facts of his life but did so in a way that showed his personality and sense of humor. (He also, ahem, parroted a portion of a famous Monty Python sketch, but I think we can forgive him.)

Writing your own obituary can be a rewarding experience, and it's far easier for you to do it—now, when you're relaxed and clear-headed—than for someone else to do it when they're grieving and under time pressure!

Obituaries tend to follow specific formats; see Writing an Obituary or Autobituary at OneWorld Memorials for a list of elements you may want to include. (Obviously, you'll leave a blank for the date of death and, unless you're terminally ill, the cause of death; your digital executor can fill these in.) Of course, you're not required to make your obituary look any certain way, and if you want to color outside the lines, this is your last chance to do so!

Please specify where and how you want your autobituary to be published. It can go in your local newspaper, of course; but keep in mind that newspapers usually charge by the line for obituaries and their rates are not inexpensive. You can also ask that it be published online (for example, as the last entry in your blog, or on the site of a family member or friend).

Genealogical and Biographical Data

So far, everything in your legacy dossier has been about you. But if you've also collected genealogical or biographical information about your family that you want to pass on for future generations, your legacy dossier is a logical place to keep a copy.

Store Your Dossier Safely and Accessibly

Just as you need to store your will in a safe place if it's to be useful when the time comes, your digital will and the rest of your legacy dossier should be stored safely—preferably, with multiple copies in different locations. Your safe deposit box is a logical place, as is a fireproof safe in your home or your lawyer's office. Wherever you put it, however, make sure your executor and digital executor know where it is and how to access it when needed.

Online Digital Legacy Services

I've found quite a few Web-based services that offer to store documents and photos, pass data on to the heirs you specify, handle certain online accounts, and in other respects function in much the same way as a digital executor. Should you consider using one?

If I believed that uploading a bunch of documents to a Web site was a great way to handle your digital legacy, I wouldn't have suggested all these other tedious steps! Although this approach *could* work well for some people, in some situations, it's far better to put your legacy in the hands of an actual human being you know and trust. I've seen a number of services like this go out of business, and I can't in good faith recommend that you entrust your entire digital legacy to a company that may not even exist when you die (see the Leave Posthumous Messages sidebar.)

Those qualifications duly given, here are some examples of sites that offer digital legacy services:

- Eterniam
- Everplans
- LegacyVault
- Planned Departure
- SafeBeyond
- SecretValet
- The DocSafe

Keep Your Dossier Up to Date

Let's say you compile the most wonderfully detailed and complete legacy dossier, but then you have the great fortune of living another 20 years. During that time, you'll be taking more photos, creating more documents, and sending more email. And, of course, anything can happen during that time—file formats and media options can come and go, your feelings about how to handle various accounts may change, and you may make different decisions about what to pass on to whom. For all these reasons, you shouldn't think of your dossier

as a static time capsule but rather as a dynamic collection of data that you'll update periodically to reflect the latest facts.

Earlier, I recommended that you Refresh Your Archives at least every 3–5 years. I now want to expand that recommendation to include your entire legacy dossier. In addition to updating your files themselves, review your digital will (especially your inventory of digital assets), your "how to be me" instructions, and everything else in your dossier and make any needed corrections or additions. And, if your digital executor should die before you, be sure to replace that person's name in your digital will! The process of refreshing your dossier shouldn't take long, and your loved ones will appreciate the effort.

About This Book

Thank you for purchasing this Take Control book. We hope you find it both useful and enjoyable to read. We welcome your comments.

Ebook Extras

You can access extras related to this ebook on the Web. Once you're on the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy a subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading on mobile devices on our Device Advice page.)
- Read the ebook's blog. You may find new tips or information, as well as a link to an author interview.
- Find out if we have any update plans for the ebook.

If you bought this ebook from the Take Control Web site, it has been automatically added to your account, where you can download it in other formats and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually:

- If you already have a Take Control account, log in to your account, and then click the "access extras..." link above.
- If you don't have a Take Control account, first make one by following the directions that appear when you click the "access extras..." link above. Then, once you are logged in to your new account, add your ebook by clicking the "access extras..." link a second time.

Note: If you try these directions and find that your device is incompatible with the Take Control Web site, contact us.

About the Author

Joe Kissell is the author of more than 60 books about technology, including *Take Control of Your Online Privacy* and *Take Control of Dropbox*. He is a contributing editor to TidBITS, a senior contributor to Macworld, and a popular speaker at conferences and other events.

When not writing or speaking, Joe likes to travel, walk, cook, eat, and practice t'ai chi. He lives in San Diego with his wife, Morgen Jahnke; their sons, Soren and Devin; and their cat, Zora. To contact Joe about this book, send him email and *please* include `Take Control of Your Digital Legacy` in the subject.

Shameless Plug

On my site Joe On Tech, I write about how people can improve their relationship with technology. I'd be delighted if you stopped by for a visit! You can also sign up for joeMail, my free, low-volume, no-spam mailing list, or follow me on Twitter (@joekissell). To learn more about me personally, visit JoeKissell.com.

Author's Acknowledgments

In the course of writing this book I benefitted greatly from discussions with Marshall Clow, who has spent more than 10 years scanning many thousands of family photos and other artifacts, and who shared his valuable insights about digitizing, naming, indexing, and preserving the media that comprise his family archive.

About the Publisher

TidBITS Publishing Inc., publisher of the Take Control ebook series, was incorporated in 2007 by co-founders Adam and Tonya Engst. Adam and Tonya have been creating Apple-related content since they started the online newsletter TidBITS in 1990. In TidBITS, you can find the latest Apple news, plus read reviews, opinions, and more.

Credits

- Publisher: Adam Engst
- Editor in Chief: Tonya Engst
- Production Assistant: Lauri Reinhardt
- Cover design: Sam Schick of Neversink
- Logo design: Geoff Allen of FUN is OK

Special thanks to Elaine Engst for her professional advice about archival materials, Marshall Clow for providing hands-on tips for managing and scanning photos, and the rest of our reviewers—Cory Byard, Norman Cohen, and Lauri Reinhardt—for sharing their insights and questions.

Image Credits

The photos at the beginning of each chapter are from the following sources:

- Envision Your Digital Legacy: Elliott Brown, "48Sheet billboard art project - Birmingham - High Street Deritend - Digbeth - My last will and testament," CC BY 2.0
- Inventory Your Digital Assets: Wikimedia Commons
- Make High-Level Decisions: Pixabay
- Digitize Photos and Documents: Pexels
- Deal with Passwords: Pixabay
- Deal with Email: Pixabay
- Deal with Social Media: Pixabay
- Deal with Other Digital Data: Pexels
- Preserve Your Data for Posterity: Ronbo76, "Old City Cemetery time capsule Sacramento, CA," CC A-SA 3.0 Unported
- Create a Legacy Dossier: Jodimichelle, "Better work flow: get organized," CC BY-SA 2.0

Copyright & Fine Print

Take Control of Your Digital Legacy
ISBN: 978-1-61542-481-8

TidBITS Publishing Inc. 50 Hickory Road, Ithaca NY 14850, USA

Why Take Control? We designed Take Control electronic books to help readers regain a measure of control in an oftentimes out-of-control universe. With Take Control, we also work to streamline the publication process so that information about quickly changing technical topics can be published while it's still relevant and accurate.

Our books are DRM-free: This ebook doesn't use digital rights management in any way because DRM makes life harder for everyone. So we ask a favor of our readers. If you want to share your copy of this ebook with a friend, please do so as you would a physical book, meaning that if your friend uses it regularly, he or she should buy a copy. Your support makes it possible for future Take Control ebooks to hit the Internet long before you'd find the same information in a printed book. Plus, if you buy the ebook, you're entitled to any free updates that become available.

Remember the trees! You have our permission to make a single print copy of this ebook for personal use, if you must. Please reference this page if a print service refuses to print the ebook for copyright reasons.

Caveat lector: Although the author and TidBITS Publishing Inc. have made a reasonable effort to ensure the accuracy of the information herein, they assume no responsibility for errors or omissions. The information in this book is distributed "As Is," without warranty of any kind. Neither TidBITS Publishing Inc. nor the author shall be liable to any person or entity for any special, indirect, incidental, or consequential damages, including without limitation lost revenues or lost profits, that may result (or that are alleged to result) from the use of these materials. In other words, use this information at your own risk.

It's just a name: Many of the designations in this ebook used to distinguish products and services are claimed as trademarks or service marks. Any trademarks, service marks, product names, or named features that appear in this title are assumed to be the property of their respective owners. All product names and services are used in an editorial fashion only, with no intention of infringement. No such use, or the use of any trade name, is meant to convey endorsement or other affiliation with this title.