

# Getting Critical Information from Tough Locations

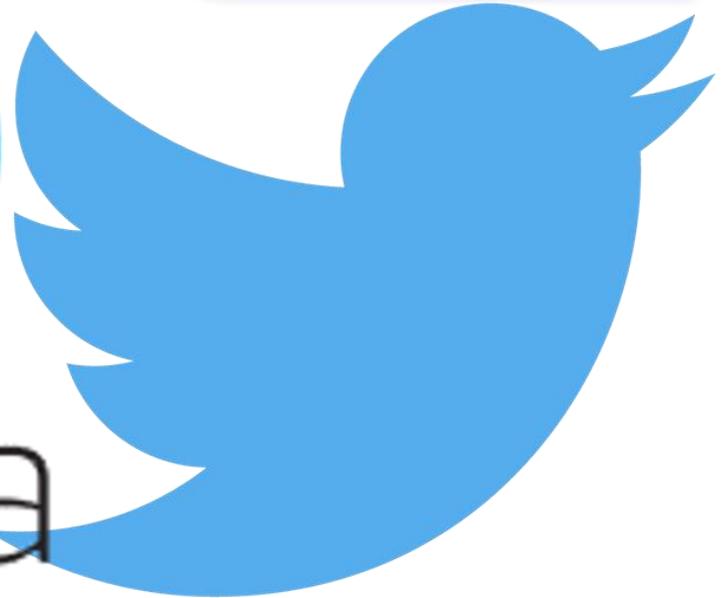
Craig Ball

© 2018

Google



alexa



## Getting Critical Information from Tough Locations

Craig Ball

©2018

I'm a lousy dancer. True, if I bite my lower lip, I can manage the arhythmic thrashing of my subspecies, *Homo sapiens caucasianus*; but where actual dance routines are concerned, I'm hopeless. People point and snicker. So, when a friend asked me to join a Thriller flash mob to dance at City Hall last Fall, prudence dictated I decline. But, New Orleans is not a place where prudence reigns (unless you mean Queen Prudence in the lavender tutu on Bourbon Street, formerly known as Bob).

I soon found myself in an Uptown ballet studio doing my best Michael Jackson moves sans chimp and anesthetic (although you could be forgiven for mistaking me for an anesthetized chimp). Our instructor made it look easy; and indeed, it *was* easy for my classmates. Kenneth would execute some swift combination of spins, dips, hitch kicks and flounces and everyone gracefully repeated them. Everyone but me that is; I struggled with everything.

Finally, I learned the critical moves; but lacking the experience that made it second nature to others, it was tough. I'm still a lousy dancer, but I'm the one back row left on the evening news last Halloween.

In e-discovery, the perception of what's tough and what's easy is likewise a function of effort and experience. It was once difficult to collect, process and produce e-mail; now it's routine. The same is true of data on personal computers and corporate servers. Today, we have standard tools and proven methods; so, it's routine.

Getting critical information from locations like mobile devices, Google and social networking sites may seem tough; yet, when you learn the steps, it's no harder than what we now regard as routine retrieval. It's all just data.

This article looks at simple no cost approaches to getting critical information from four data sources deemed tough locations in e-discovery: **Google** (including **Gmail**), **Facebook**, **Twitter** and the **Amazon Alexa App**. An accompanying article details a simple, scalable and no-cost methodology for preservation of iPhone data.

You could criticize any of the approaches here for one reason or another, and all warrant scrutiny in order that we might always seek better ways and better evidence. Still, we shouldn't let perfect be the enemy of good enough. If the alternative to using a good enough method is ignoring the evidence or being forced to rely on methods too costly and disruptive to be proportionate, good enough methods that get the evidence beat the pants off perfect methods no one uses.

### Google Takeout

Like a billion others, I depend on Google apps (like Gmail and Google Calendar) and have for a dozen years. As an expert witness, I collect and produce messages and attachments in response to subpoenae *duces tecum*. Gmail made it easy to *find* responsive content, but hard to get that content out in forms that preserved utility and integrity. In the past, I'd printed the items to searchable PDFs; but, printing to PDF is tedious and runs counter to my penchant for functional and complete native forms.

For years, I used the IMAP protocol to download Gmail to Outlook, creating .PST container files and processing these with e-discovery tools. Getting a complete, compact PST is no picnic. It can take days to grab all message headers, message bodies and attachments from big collections, and the level of replication is appalling because, when they downloaded using IMAP, messages in folders (i.e. labeled messages) yield duplicate messages and attachments for each label applied. The upshot is that anything

in, say, the Inbox or Sent Mail folders also shows up in the All Mail group. This is a convenience online; but, radically increases the collection time and storage required to pull the data out with IMAP. Message threading is also a casualty when converting Gmail to Outlook content.

Historically, you had two choices when it came to putting Gmail on legal hold: Either you'd instruct your client not to delete anything (and cross your fingers they'd comply) or you had to hire someone to download the data. Now, Google does the Gmail collection *gratis* and puts it in a standard [MBOX container format](#) that can be downloaded and sequestered. Google even incorporates custom metadata values that reflect labeling and threading. You won't see these unique metadata tags if you pull the messages into an e-mail client; but, capable e-discovery software will pick them up. I tested this using [Nuix](#) and it parsed the Gmail metadata handily, enabling the messages to be threaded and paired with their Gmail labels.

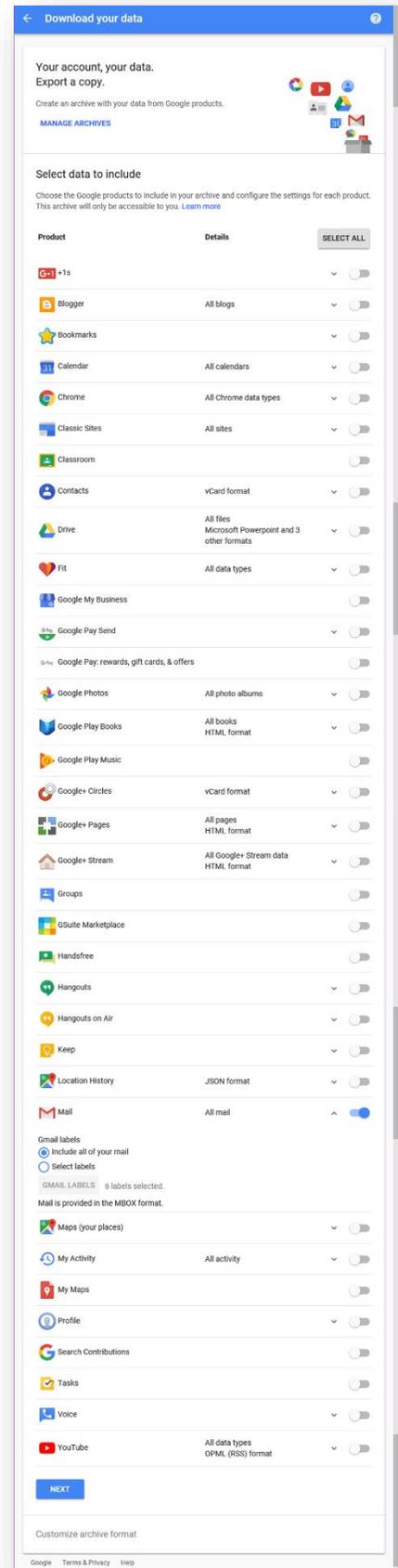
MBOX might not be everyone's choice for a Gmail container file; but, it's inspired. MBOX stores the messages in their original Internet message format called RFC 5322. I've been a vocal proponent of this format as superior for e-discovery [preservation](#) and [production](#). I had no hand in Google's decision; but, it's nice to have Google on my side!

So, let me introduce you to [Google Data Tools](#) a/k/a **Google Takeout**.

***NOTE: Collecting a user's Google data necessitates the ability to log into the user's Google account and access to the user's Gmail to obtain a download link that will be sent when the data is ready for retrieval. Alternatively, Google takeout collections may be delivered to Drive, Dropbox or OneDrive accounts.***

The hardest part of collecting Google data is navigating to the right page. You get there from the Google Account Setting page by looking for "Download Data" and clicking on "[Select account data to download](#)." You'll see a menu like that at right where you choose what Google content to download. For Gmail, you can select whether to download all mail or just items bearing the labels you select.

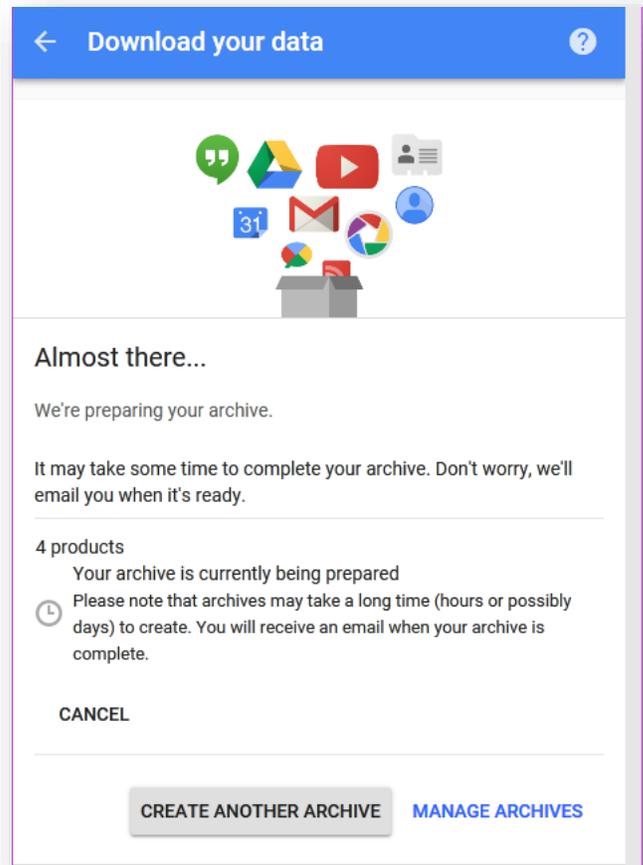
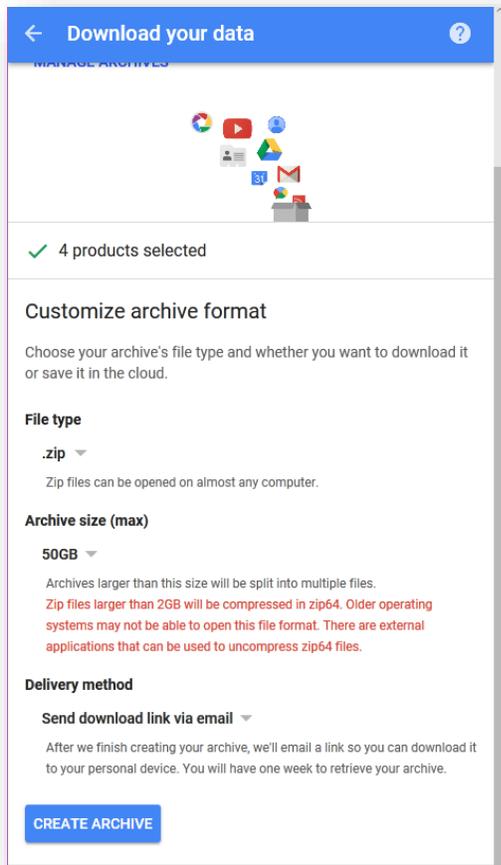
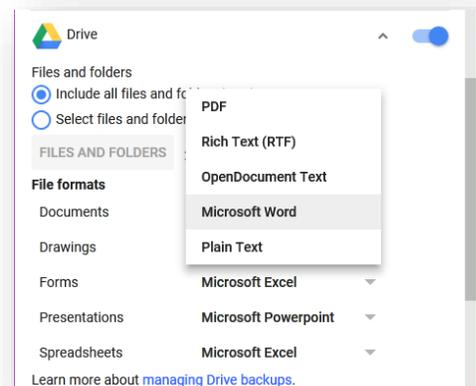
The ability to label content within Gmail and archive only messages bearing those labels means that Gmail's powerful search capabilities can be used to identify and label potentially responsive or privileged messages, obviating the need to collect everything. It's not a workflow



suited to very large cases; yet, it's a promising capability for keeping costs down in cases involving a handful of Gmail users.

Most of the Google products listed permit the scope of the archive to be customized when selected for download. For example, taking out an archive of a user's Google Drive account allows for filtering by file formats (see figure right).

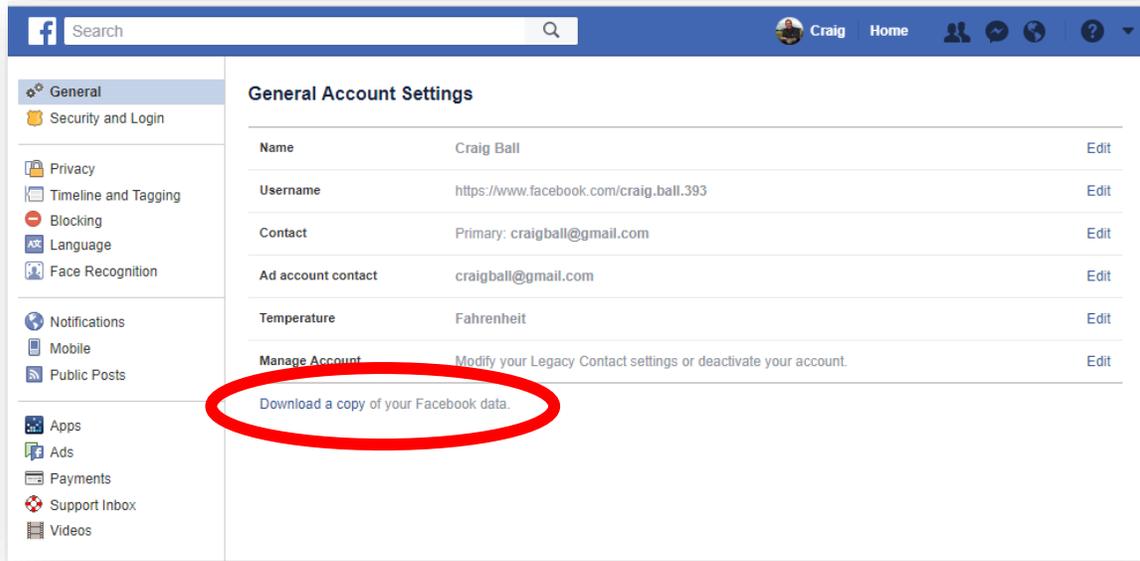
The Google takeout tool allows for choice of file compression (Zip or TGZ) for the deliverable, along with specifying the maximum file size before the archive is split into multiple containers and the delivery method (e-mail link, Drive, Dropbox or OneDrive).



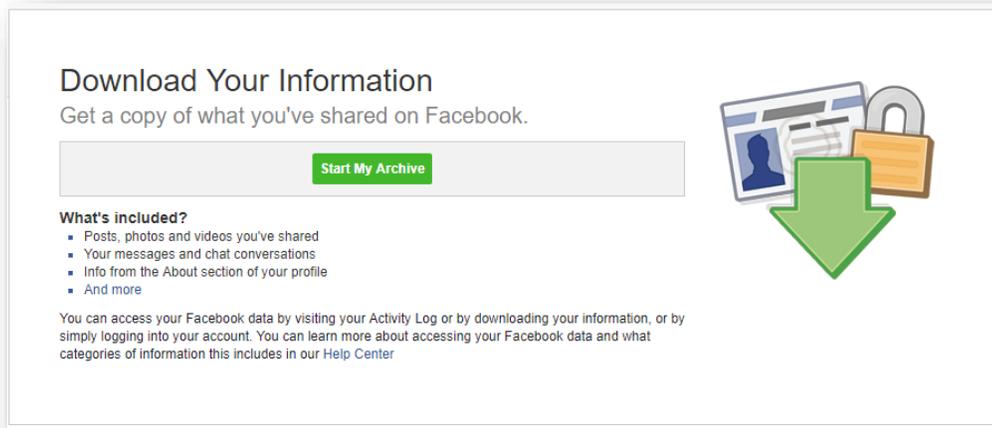
## Facebook Archive

Facebook permits users to download a copy of much of their Facebook data by logging into the account and navigating to [Settings>General Account Settings](#) and clicking on "[Download a copy](#) of your Facebook data."

**NOTE: Collecting a user's Facebook data necessitates the ability to log into the user's Facebook account and access to the e-mail account linked to the user's Facebook account to obtain a download link that will be sent when the data is ready for retrieval.**



The link will lead to the Download Your Information page seen below. Click Start My Archive and Facebook will require the account password be re-entered. Note the hyperlinked text "And more" under What's Included? It links to a huge table describing the data in the archive.



When the archive is ready, the user receives an e-mail notification containing a download link. You can also retrieve the archive by navigating back to the Download Your Information page. The "Start my Archive" button will now read "Download Archive."

The extent and variety of a user's Facebook data available for download has grown over time and is staggering and shocking for those unaware of how much data Facebook collects. In my case, the archive

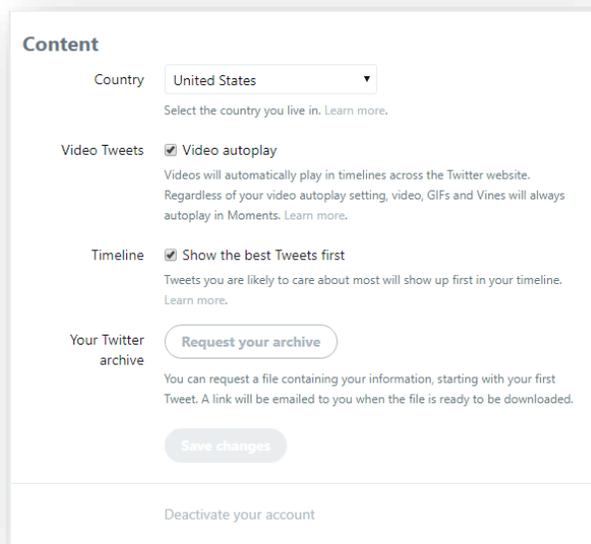
held years of data on Facebook sessions (including IP addresses), hundreds of photos and videos (many containing geolocation coordinates) and a decade of activity, posts and messages.

The archive arrives as a compressed Zip file. When extracted to a folder it can be viewed using a browser from a supplied index page, just like a website. Photos, videos and messages are discrete files in separate folders, all very easy to navigate.

### Twitter Takeout

It takes only a couple of clicks to collect a user's tweets. After logging into the account, click on the Profile and Settings link in the upper right corner of the page (mine uses my photo as the link button) or go to <https://twitter.com/settings>. Choose "Settings and Privacy" from the drop-down menu and in the Content section of the Settings page, click on "Request your archive" (see figure at right).

**NOTE: Collecting a user's tweets necessitates the ability to log into the user's Twitter account and access to the e-mail account linked to the user's Twitter account to obtain a download link that will be sent when the data is ready for retrieval.**



When the archive is ready, the user receives an e-mail notification containing a download link. The archive arrives as a compressed Zip file. When extracted to a folder, it can be viewed using a browser from a supplied index page, just like a website.

### Amazon Alexa History

In March of 2016, I [blogged](#) about the challenge of seeking to preserve records of interactions with the Amazon Echo/Alexa family of devices and applications. I concluded:

*"Listen, Amazon, Apple, Microsoft and all the other companies collecting vast volumes of our data through intelligent agents, apps and social networking sites, **you must afford us a ready means to see and repatriate our data.** It's not enough to let us grab snatches via an unwieldy item-by-item interface. We have legal duties to meet, and if you wish to be partners in our digital lives, you must afford us reasonable means by which we can comply with the law when we anticipate litigation or respond to discovery."*

In a testament to my thought leadership, nothing whatsoever has happened since my call-to-arms in terms of the ability to preserve Alexa app history data. It's as bad as it was two years ago and arguably worse because Echo products have grown so popular and the Alexa interface has been integrated into so many devices that the problem is bigger now by leaps and bounds.

Don't get me wrong, I am Alexa's biggest fan (and adore her sisters, "Amazon" and "Computer," so-called for the alternate "wake words" I use to trigger voice communication to Amazon's servers from other Echo devices). If anything, Craig the Consumer is happier now with the Echo ecosystem than two years ago. Wearing my user hat, Alexa's a peach (and, yes, I am perfectly comfortable with her from a privacy

point of view). Wearing my e-discovery propeller beanie, Alexa is a pain in the butt. She's a data gold digger who cooks the books to make it supremely difficult to account for what she's taken.

Granted, the Alexa app used to manage and monitor Alexa accounts offers a long "history" of interactions with Alexa in all her myriad manifestations (Settings>Alexa Account>History). Tragically for those seeking to preserve this historic data, the interface is unwieldy and time-wasting. I doubt they could have done worse if they'd set out to create a nearly-useless interface.

For example:

1. There is no way to download the historic data or request it be supplied in a containerized format à la Facebook and Google's Takeout. [Put aside using a subpoena as we are speaking of custodial-directed preservation of one's own data, often before suit].
2. Within the Alexa app, you cannot search or filter the history of voice interactions with Alexa. The only way to navigate the history (and make earlier history data visible and accessible) is to scroll down screen-by-screen, at a rate of about 15 transactions per screen. You can't go directly to the end (oldest records), or search for an entry by text or date. You can't see content "below the fold" without painstakingly shoving the scroll bar down, down, down, DOWN for (in my case) over *700 screens*—minutes of tedious scrolling to reach December of 2015.
3. Clicking on any entry in the history to examine it necessitates starting the whole tedious scrolling operation *again*. Clicking "back" in your browser doesn't return you to where you left off in a list of thousands of entries. This is a big deal because you can't see what response Alexa supplied or listen to the voice recording without clicking into each entry. Yet, after clicking on any entry, *you must scroll starting from the top, all over again, to get back to where you were*. Imagine reading a book where you can't turn to the next page *without perusing every prior page again-and-again*. Now, imagine you must find where you left off without page numbers. It's maddening.
4. The data isn't delimited, meaning that it's not fielded for retrieval or sorting. It's undifferentiated text without a means to uniquely identify each record apart from its date.

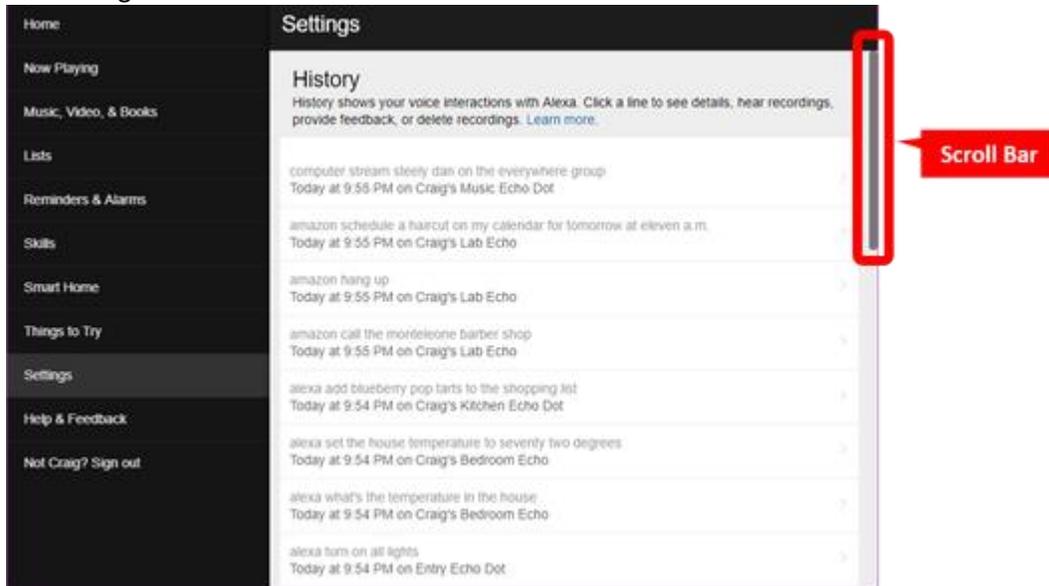
It would be simple, even trivial, for Amazon to make delimited history data readily downloadable in an easy-to-use format. But Amazon hasn't done so, and a litigant's duty to preserve ESI when its potentially relevant doesn't disappear when collection isn't pushbutton easy.

So, I sought an easy, no-cost way to preserve aggregate Amazon history data—an inelegant method to tide us over until Amazon gets on the stick or someone builds a better collection tool. I'll concede my approach isn't pretty; but, its dead simple and requires no special software or expertise.

With Echo history data, defensible preservation may allow for doing nothing. Amazon's History page in the Alexa app retains transactions until deleted; so, if you can be confident that entries won't be deleted by the user or overwritten by Amazon, you can preserve them by leaving them alone: deleting nothing and insuring the account stays open.

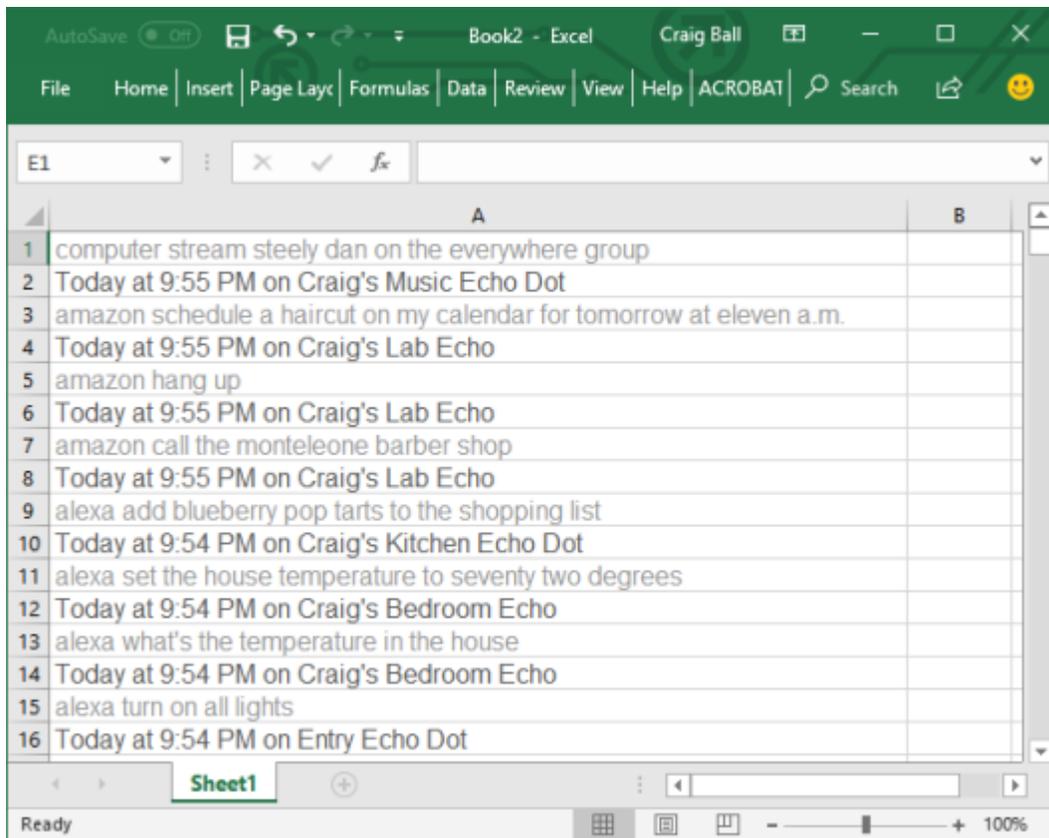
But, if you must guard against the foreseeable risk of loss or simply deflect suspicion of same, you will want to duplicate and sequester Alexa history data. If you intend to electronically search an extensive Alexa history or bring it into a review tool, you have little recourse but to collect the contents in a searchable format. Forget screenshots for this; they aren't text searchable and capturing 700 screenshots will turn a healthy brain to mush.

To start, let's examine the History interface in the Alexa app (which can be accessed on a phone or via a Windows computer). I find it's easier to preserve History data using a computer and mouse. Login to the Alexa account via <https://alexa.amazon.com>. Navigate to Settings>Alexa Account>History. You will see something that looks like this:



If you enter CTRL-A now, all the content on the page would be selected. If you enter CTRL-C all the selected content will be copied. But, the copied data would consist solely of the data seen on the screen, and none below. As noted, some 700+ additional screens follow this one; *but, the browser won't retrieve that content until the scroll bar is pulled down to make the other screens visible*. As the scroll bar is pulled down and historical data retrieved, ALL the data retrieved, *including all that was briefly visible as you scrolled through it*, is buffered and can be selected and copied. **So, if you scroll all the way to the earliest content (at the final, "bottom" screen of the scroll), you can then use CTRL-A (select all shortcut) and CTRL-C (copy all shortcut) to select and copy the entire contents of the history that appeared while scrolling.**

Put simply, if I have 700 screens of history to scroll through, once I have done so, I can select **all** the scrolled data and copy it to the Windows clipboard. Now, I can paste the data into a file or application for preservation. Better yet, if I paste the copied data into an Excel worksheet, the data easily converts to delimited formats. The commands and the dates and devices when and where the commands were heard will occupy alternating cells, with the commands appearing in odd-numbered rows and the dates, times and devices in even-numbered rows. Like so:

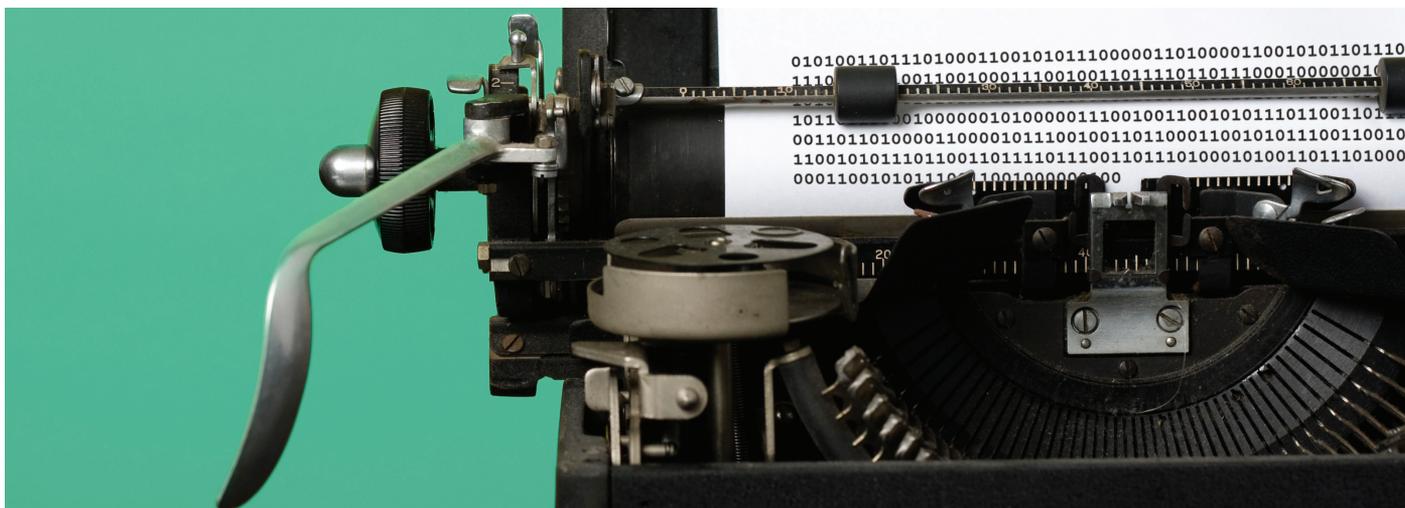


Putting the data in a spreadsheet makes it instantly text searchable. With some minor massaging, you can restructure the data as a load file suitable for ingestion by an e-discovery review platform.

Is this an elegant or complete preservation solution? Far from it. It's pretty lousy. It doesn't collect the audio recordings of the spoken commands nor the responses supplied by Amazon, both available one-by-one, by clicking through individual entries; but, not currently retrievable apart from plodding manual methods. All that can be said of this solution is that, in its crude way, it works, and is better than nothing. For the moment, "nothing" appears to be its sole competitor.

### **Not So Tough**

Four simple methods to collect critical evidence. No IT expertise required. No special software tools needed. And it didn't cost a dime. In routine e-discovery settings, you can defend each as a reasonable, proportional means of data preservation. *Perfect for every case?* No. *Good enough in most cases?* Absolutely!



small\_frog/Getty Images

# Back It Up: Custodian-Directed Preservation of iPhone Data

Mobile devices have evolved to capture significant volumes of data and are a vital source of evidence. However, litigants often argue that data stored on mobile devices is too expensive or burdensome to preserve and collect at scale. Putting a protocol in place for custodians to back up their iPhones can easily mitigate these issues and make custodians less inclined to fight or subvert the preservation process.



## CRAIG D. BALL

PRESIDENT  
CRAIG D. BALL, P.C.

Craig is a trial attorney, certified computer forensic examiner, and e-discovery consultant who frequently serves as a court-appointed ESI special master. He authors *Ball in Your Court*, an influential blog on e-discovery. Craig is also an adjunct professor at The University of Texas at Austin School of Law, where he teaches an e-discovery and digital evidence course.

Mobile device applications (apps) are the principal conduit for individuals to access online information, eclipsing the use of laptops and desktops in recent years. People increasingly have their most candid conversations through text messaging (texts) rather than email. App data and texts reside primarily, and often exclusively, on mobile devices. Indeed, mobile devices are where modern evidence lives, yet parties frequently fail to preserve mobile data in litigation.

Best practices in preservation require in-house or outside counsel to send a legal hold notice instructing custodians to take steps to preserve potentially relevant electronically stored information (ESI). This custodian-directed preservation method has been criticized for requiring custodians to make judgments concerning relevance, materiality, and privilege, and for the other inherent risks of self-collection. Hold notices typically require custodians to refrain from taking any action that might disturb or destroy potentially relevant ESI, forcing litigants to

engage litigation technologists who are qualified to collect ESI in a defensible manner.

However, custodian-directed preservation can be efficient and cost-effective, and plays an important role within a larger, defensible preservation protocol. For example, backing up an iPhone is a simple, quick, and comprehensive process. It offers litigants a proportional and verifiable method to collect ESI, without requiring custodians to part with their devices even temporarily. Crucially, after creating backup files, it is exceedingly difficult for a custodian to omit or alter the ESI.

This article guides counsel on how to incorporate a custodian-directed iPhone backup technique into a preservation and collection protocol. Specifically, it provides:

- A rebuttal of common arguments against preserving mobile data.
- An overview of the advantages of custodian-directed preservation by backup, including information on proportionality and defensibility.
- An explanation of the iPhone backup process using Apple iTunes (a free program for PCs and Macs), including details on how to compress backup files and store them on external media.
- A model iPhone preservation directive that counsel can send to custodians when using a custodian-directed preservation process.

## MISCONCEPTIONS ABOUT MOBILE DATA PRESERVATION

Some litigants choose not to preserve any data rather than use methods that preserve some, but not all, potentially probative ESI from mobile devices. Litigants who fail to meet their duty to preserve unique and relevant mobile data often attribute their failure to:

- **Company policies barring business use of smartphones.** This argument is unpersuasive because, by itself, the existence of a policy that bars the use of mobile devices to store relevant data is insufficient to prove that these devices were not actually used to store relevant data. Courts often weigh the actual practices used by company employees more heavily than corporate policies, particularly regarding employee text messaging.
- **The cost-prohibitive nature of forensic technologies needed to preserve and collect mobile data.** Absent issues of spoliation, few matters warrant the added cost of mobile data preservation by forensics experts or the burden and disruption of separating users from their mobile devices.
- **The personal privacy and privilege concerns implicated by mobile data.** The case law is clear that even legitimate concerns about personal privacy and privilege do not justify a custodian's failure to preserve relevant mobile data. However, privacy concerns may be expected to play a key role in a litigant's approach to data processing, searching, review, and production.

## ADVANTAGES OF PRESERVATION BY BACKUP

As noted above, custodian-directed preservation is often criticized for the risk that a custodian will overlook or deliberately omit relevant materials. Custodians also may lack the necessary time, tools, or training to successfully search for and preserve ESI. A mobile device backup approach mitigates these shortcomings and, when paired with other steps like IT-initiated and counsel-supervised holds, ensures that the custodian-directed preservation process is both:

- Scalable and proportional, given the issues raised in the case.
- Defensible, in that it is capable of being audited and verified.

## SCALABILITY AND PROPORTIONALITY

Scalability describes the ability of a system or process to handle a growing number of tasks or a larger volume of data. While scalability is a crucial consideration in all phases of e-discovery, it is particularly challenging when dealing with mobile data. Historically, preserving mobile data was a one-off task, seldom undertaken and typically needed for only a handful of devices. Using a digital forensics specialist to image the contents of a single phone to preserve its contents was the norm and, though costly, the obligation rarely had to scale to dozens or hundreds of far-flung devices. For one or two phones, a litigant could complete the preservation in a few days for about \$1,000.

However, once a litigant must preserve ESI from numerous phones in distant locations, the time, cost, and disruption caused by using digital forensic experts and requiring custodians to temporarily relinquish their phones becomes untenable. Accordingly, many litigants opt not to preserve the content of mobile devices, typically claiming (absent compelling contrary evidence) that the phones do not hold relevant data. Moreover, these objections often suggest that collection from these mobile devices would be unduly burdensome, even without providing supporting metrics.

The backup process is inexpensive and scales easily for phones and tablets (see below, *Sample iPhone Preservation Directive*). This custodian-directed preservation method:

- Minimizes business disruption because custodians do not have to part with their devices.
- Is speedy.
- Does not require custodians to make judgments concerning relevance, materiality, or privilege.
- Poses almost no risk of loss or alteration of the relevant data and is unlikely to prompt custodians to game the process.
- Does not require special tools, cabling, software, or technical expertise.
- Avoids any operating system compatibility issues.

In short, the cost and burden of custodian-directed iPhone preservation are sufficiently trivial that relevance alone should be the guiding star in deciding whether to preserve mobile data.

## DEFENSIBILITY, AUDITABILITY, AND VERIFICATION

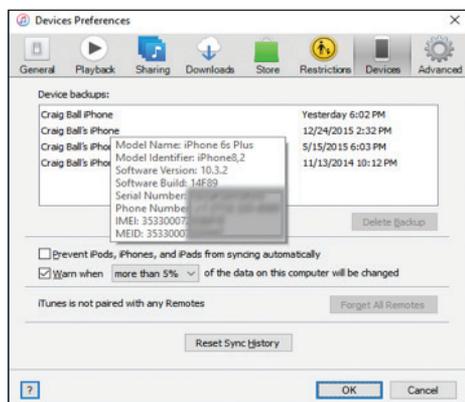
Audit and verification information is important when an opposing party questions a litigant's preservation practices. This type of information can show the defensibility of a litigant's preservation and collection processes by, for example, providing a chain of custody for a particular type of media and a record of the type of ESI that was preserved and collected, and by whom.

There are several ways to audit and verify a custodian-directed preservation effort to demonstrate the defensibility of a litigant's preservation process. In selecting an optimal method, the litigant should consider the likely grounds for and sophistication of challenges to the integrity of the evidence. The recently-amended Federal Rule of Evidence Rule 902(14) offers a ready means to defeat attacks on the authenticity of preserved data through the use of cryptographic hashing and certifications (with notice). For example, a custodian can create an audit trail using:

- **A screenshot of the details panel for the latest backup.** As shown in Figure 1, a custodian can take a simple screenshot (using Alt-Prnt Scr) when hovering over the relevant backup record in "Devices Preferences" in iTunes.
- **Cryptographic hashing.** A hash value is a sequence of characters produced by an algorithm and calculated from the digital contents of a storage medium, file, or collection of files. It serves as a digital fingerprint of the data. Different data sets produce different hash values, and matching hash values are highly probative of identical data. Therefore, obtaining a hash value of data when acquired simplifies the task of proving that the data was not subsequently altered in any way. Free applications to compute hash values are readily available and easy to use.
- **Remote screen-sharing and screen-recording software.** This approach affords a sponsoring witness or designee step-by-step oversight of the entire process. Screen-sharing capabilities are built into most computers and available as free and low-cost online services. The observer can attest that the custodian fully and correctly acquired the data on the mobile device or, if afforded remote control, can initiate and supervise the process from anywhere.

Additionally, iPhone backup sets may be sampled and tested for accuracy and completeness.

Figure 1



## MECHANICS OF IPHONE BACKUP

Custodian-directed preservation of iPhone data is usually a one to two hour process that involves:

- Creating a backup of an iPhone using iTunes.
- Saving the backup to external storage, if there is insufficient storage on the computer the custodian uses to create the backup.
- Compressing the backup file.

## ITUNES VERSUS ICLOUD BACKUPS

When collecting iPhone data, a litigant may choose to preserve using either a backup from iTunes or from iCloud. An iTunes backup provides several advantages over iCloud from a preservation perspective.

### iTunes

iTunes offers both encrypted and unencrypted backup options. Depending on the type of data that is likely relevant, a litigant may prefer one method over another. As a practical matter, it is impossible to process an encrypted backup without user credentials. Moreover, some tools cannot process the contents of encrypted backups even with credentials. For these reasons, it is often preferable to collect the data as an unencrypted backup and obviate the need for credentials.

Litigants should be aware that neither encrypted nor unencrypted iTunes backups include email stored on an iPhone. Additionally, unencrypted iTunes backups do not include:

- Passwords.
- Browsing histories.
- Wi-Fi settings.
- Content from the iTunes and App Stores.
- PDFs downloaded directly to iBooks.
- Content synced from iTunes, like imported MP3s or CDs, videos, books, and photos.
- Photos already stored in the cloud, like My Photo Stream and iCloud Photo Library.
- Touch ID settings.
- Apple Pay information and settings.
- Activity, Health, and Keychain data.

By contrast, encrypted iTunes backups preserve activity, health, and keychain data and Wi-Fi settings.

To protect the data and add efficiency, technologists typically compress and encrypt the backup set using credentials chosen for the legal hold project, rather than using each custodian's credentials. If some of the data that would be captured by an encrypted backup but would not be captured by an unencrypted backup is particularly relevant to the case, a litigant should either:

- Identify an alternative means of preserving that content.
- Proceed with an encrypted backup, select a processing tool that can handle it, and be sure to acquire and maintain the necessary credentials.

### iCloud

Unlike iTunes backups, iCloud backups permit users to back up data from their phones to their iCloud accounts wirelessly. Depending on a user's settings, an iCloud backup can be made either manually or automatically when the device is plugged in, locked, and connected to Wi-Fi.

Despite the convenience of an iCloud backup, it preserves less data and requires more time to create than an iTunes backup. Additionally, because iCloud encrypts all backups, these backups tend to present processing and search challenges later in the workflow if a user's credentials become unavailable. Finally, iCloud backups are dynamic, changing frequently and making them difficult to authenticate to a point in time or by hashing.

### COMPRESSING THE BACKUP FILE

Compressing the backup to a Zip file makes it easier to transmit or copy the backup to new media. Depending on the composition of the backed up data, the compressed Zip file may be much smaller or similar in size to the uncompressed iPhone backup. For example, much of the data on a typical iPhone consists of JPEG photos that are already in a compressed format. This already-compressed data tends not to compress because there is little "space" to squeeze out by further compression.

However, preserving data in a Zip file guards against the potential risk that a subsequent backup of the iPhone will overwrite the data. Additionally, depending on the Zip tool used to compress the file, the Zip process affords a means to securely encrypt the data without having to install an encryption tool.

Any Windows machine can create compressed and encrypted Zip files, as well as any Mac running OS X. Counsel may wish to instruct each custodian to encrypt the backup using a password chosen for the legal hold project instead of each custodian's personal password.

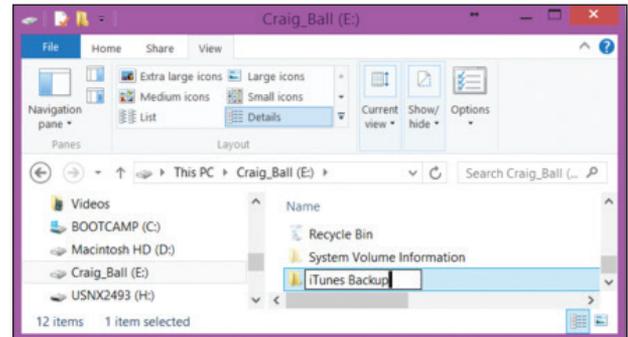
### REDIRECTING THE BACKUP FILE TO EXTERNAL MEDIA

Given the vast stores of ESI on an iPhone, an iTunes backup may fail to complete because there is not enough free space available on the computer performing the backup. A custodian may be able to resolve this by emptying the computer's Recycle Bin. However, if a custodian cannot clear enough space on the C: drive (the default location for an iTunes backup), the custodian can instead "trick" a Windows machine into storing the backup on a sufficiently sized alternate or external storage medium.

To address this situation, a custodian can redirect an iTunes backup location in Windows using the following steps:

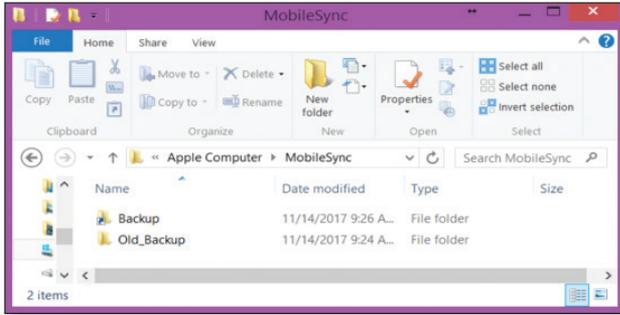
- **Create a new backup folder.** The folder should be on a disk with sufficient space to create the backup (roughly twice the capacity of the iPhone is sufficient). In Figure 2, the new iTunes backup location on the E: drive was named "iTunes\_Backup."

Figure 2



- **Rename the current iTunes backup folder.** By default, the iTunes backup folder is located at the following filepath:  
`C:\Users\custodian account name\AppData\Roaming\Apple Computer\MobileSync\`  
 The *custodian account name* is the name of the Windows User ID on the computer. The custodian can right click on the "Backup" folder and rename it (for example, "Old\_Backup").
- **Redirect the old backup folder address to the newly renamed one.** To complete this step, the custodian must use a Windows Command line interface. Given the potential for mistakes in this step, the custodian should write down the full filepaths to both the old and new backup folders. Both must be correct for the redirection to work. The old one should be:  
`C:\Users\custodian account name\AppData\Roaming\Apple Computer\MobileSync\Backup`  
 The new path is on whatever storage medium the custodian selected and will follow the filepath and folder name the custodian gave it in the first step (the example uses "E:\iTunes\_Backup").
- **Open a command prompt window.** To open a Windows command prompt interface, the custodian can either press the Windows key and then type "cmd" and press Enter or press the Win + R keys on the keyboard then type "cmd" and Enter. At the command line, the custodian should carefully type the following command:  
`mklink /J "[path to old backup location]" "[path to new backup location]"`  
 The bracketed text should be replaced with the old and new paths the custodian recorded in the previous step (no brackets). The custodian must be sure to enclose each path in quotation marks, as shown. The command and response might look like the image in Figure 3.

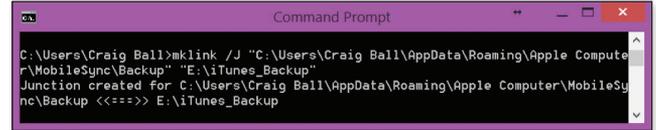
Figure 3



The mklink /J command creates a Windows symbolic link or “directory junction” that will redirect any actions that would have been performed on the old backup folder to the new one. To test the effect, the custodian can double-click on the backup folder in MobileSync, which will direct to the

new backup folder. When looking at the MobileSync folder (C:\Users\custodian account name\AppData\Roaming\Apple Computer\MobileSync), the custodian will see a folder shortcut named “Backup” alongside the renamed old backup folder as shown in Figure 4.

Figure 4



- **Run the iTunes backup.** The custodian must confirm that the media selected to hold the relocated backup is attached to the computer. After that confirmation, the custodian can run the iTunes backup as usual.

**SAMPLE IPHONE PRESERVATION DIRECTIVE**

Counsel can use the following sample letter when drafting an iPhone preservation directive to a custodian. Counsel may also include a modified version of this sample when making a preservation request to an opposing party or a third party to direct these parties to preserve mobile data.

Counsel should customize the language to suit the needs of the case and controlling law and, because iTunes changes its internal menus and appearance periodically, counsel should consult the most recent version of iTunes and make appropriate modifications to the sample text as needed.

This sample omits optional steps a custodian can take to encrypt the data set and transfer the backup to an external repository for preservation, as these steps are frequently unnecessary to meet preservation duties. It includes optional language in bracketed text for personally owned but company-enabled iPhones.

This sample assumes that the recipient has previously received a legal hold notice describing other preservation obligations.

Dear [Custodian]:

You recently acknowledged your obligation to preserve information relevant to a dispute between our company and [OPPOSING PARTY]. Please see the hold notice dated [DATE OF LITIGATION HOLD] for further details.

Within **48 hours of your receipt of this notice**, you must preserve the contents of your [company-issued/personally owned and company-enabled] iPhone (the “iPhone”). If you cannot comply, please advise me at once by email or phone. **Time is of the essence.**

By following the step-by-step instructions below, you will make an unencrypted backup using iTunes and compress the backup folder. **You must carefully follow the procedures set out below.** Do not assume that you have been:

- Automatically creating an unencrypted backup of the data on the iPhone.
- Preserving all necessary data by using iCloud as a backup.

**PREPARATION**

You will need:

- The iPhone and its USB charge/sync cable.
- Your company-issued desktop or laptop computer with the iTunes program installed.

The computer must have available storage space on its boot (C:) drive that has twice as much the storage capacity as the iPhone. For example, if the iPhone has a 128GB capacity, the computer must have at least 256GB of unused storage space on its C: drive. You can find the capacity of the iPhone in Settings>General>About>Capacity. You can find the available storage on your computer's C: drive using File Explorer on a Windows machine or Finder on a Mac.

### TIME REQUIRED

The backup and compression process will take approximately one to two hours (most of it unattended "machine" time).

It will take about 10 to 15 minutes to follow these instructions, update iTunes (if needed), and begin the backup. The backup will be created in less than 30 minutes and you can continue to use the iPhone during the backup process, as long as you do not disconnect the charge/sync cable.

It should take less than one hour to compress the data and about ten minutes to confirm that the backup was successfully compressed and to report on the results. So long as the computer is secure and powered up throughout the process, you do not need to supervise or leave the iPhone connected once the backup completes.

### INSTRUCTIONS

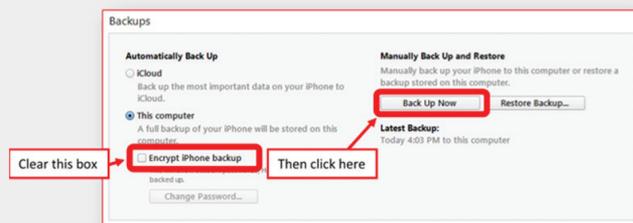
1. Open iTunes and check for updates (Help>Check for Updates). If not already installed, install the latest version of iTunes.
2. Connect the iPhone to a USB port on the computer using a USB charge/sync cable.
3. If a message asks for the device passcode or to Trust This Computer, follow the onscreen steps.
4. Select the iPhone when it appears in iTunes, as shown in Figure A. Click "Summary" in the sidebar.

Figure A



5. In the Summary pane, uncheck "Encrypt iPhone Backup," as shown in Figure B. Then click "Back Up Now." You need not otherwise modify the backup settings on the iPhone.

Figure B



6. Monitor the progress of the backup at the top center of the iTunes window. After the process ends, check if the backup finished successfully:
  - **iTunes for Windows.** Choose Edit>Preferences>Devices from the menu bar at the top of the iTunes window.
  - **iTunes for Mac.** Navigate to iTunes Preferences>Devices.

In both Windows and Mac, you should see the name of your device with the date and time that iTunes created the backup. If you see this icon  beside the name of your device, you must repeat steps one through five until you do not see  beside the name of your device. Specifically, confirm that the “Encrypt iPhone Backup” option is not checked.

7. Disconnect the iPhone from the computer.

8. Locate the backup folder:

- **Windows.** Using File Explore, navigate to: C:\Users\*your account name*\AppData\Roaming\Apple Computer\MobileSync\Backup\. Note that “*your account name*” is the name of the Windows User ID on the machine.
- **Mac.** Using Finder, select Go>Go to Folder on the Finder menu and enter: ~/Library/Application Support/MobileSync/Backup/

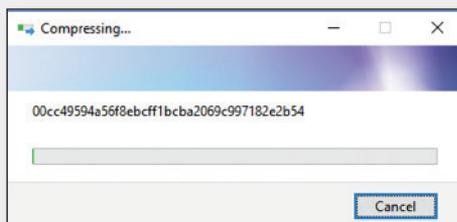
In both Windows and Mac, the backup folder will contain one or more subfolders with 40-character names (for example, “12da34bf5678900386c48267658d340eb34007f8”). If there are multiple subfolders, identify the subfolder that has the time and last modified date that matches the time you started the backup process.

9. Compress the contents of the subfolder:

- **Windows.** Right click on the subfolder just identified and select “Send to>Compressed (zipped) folder.” A progress panel like the one shown in Figure C should appear.
- **Mac.** Right click on the subfolder and select “Compress.”

Do not turn off your computer or reboot while the compression process completes. It should take less than one hour to complete the compression process, depending on the type and volume of data being backed up.

Figure C



10. Once the compression process has completed, in both Windows and Mac, navigate again to the backup folder (see step 8 above) to confirm the presence of a file with the same name as the subfolder you identified but with the file extension “.zip.” Record the name, date/time, and size of the Zip file. If you cannot see file extensions on your Windows machine, open “My Computer,” click “Tools,” and click “Folder Options,” or click “View” and then “Options,” depending on your version of Windows. In the Folder Options window, click the “View” tab. Uncheck the box that says, “Hide file extensions for known file types.” This should make file extensions visible.

11. Send the name, date/time, and size of the Zip file you just created to the undersigned at the email address listed below. Do not delete or open this file. It must be preserved without alteration until further notice.

Your supervisor is copied here to ensure you are afforded the time, oversight, and support needed to comply in a timely way. Thank you for your cooperation. Call me at [TELEPHONE NUMBER] with any questions.

Best regards,

[NAME]

[EMAIL ADDRESS]