Time Traveling Bandits - Keeping Your History Safe

Michael Stringham: mstringham@gmail.com
Roselle Harney: roselleharney@gmail.com

1. Virtues and Pitfalls of Online Data
    a. Virtues:
        i. Safe from local disasters
        ii. Accessible anywhere
        iii. Easily shared with others
        iv. Instant collaboration
        v. Visualize data
        vi. Multimedia
    b. Mind the "Historical Gap"
        i. missing data in your historical timelines, due to: forgetfulness, carelessness, corruption, theft, unknown

    c. Pitfalls:
        i. Data can be hacked or stolen
            1. There are cases of this worldwide, almost weekly
        ii. Data providers become obsolete
        iii. Family History sites are not immune!
        iv. Lack of privacy
2. Records and Resources in hand, at home, or abroad
    a. The "Archive Matrix" - Store your data in multiple locations!
    b. At home:

	HOME	
	Paper	**Digital**
5 min	In a safe, Fireproof box or envelope	Thumbdrive
5 hours	Books, albums	CD, DVD, Blu-Ray, Quick Scanning, Audio & Video Recordings
5 days	(Re)Organization efforts, in-store photo service	Multimedia Recording, Editing, Storage
5 months	Family Pictures, Scrapbooking, Print Pedigrees, Charts, Mail-in photo services	Organize family photos, videos, touch-ups, create long-term backups
5 years+	Compile family history books, Journals, Review integrity of artifacts	Assess archival media, replenish as needed

        i. Store important or sensitive documents in a safe place
        ii. Keep your personal data secure: https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure
        iii. Scanning: http://genealogysstar.blogspot.com/2014/05/free-scanning-service-offered-at-family.html
        iv. Digital Conversion Services: https://www.larsendigital.com/services.html
        v. Image Format Considerations: http://shutha.org/node/828
        vi. Preserving Photos: https://familysearch.org/blog/en/helping-photographs-live/
        vii. Data loss is not just concerned with loss of files. It's a loss of efforts, money and time.
        viii. Remember: How valuable is each piece of data?
        ix. Carry copies of less important documents with you
        x. Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar documents when you don't need them any longer.
        xi. Destroy the labels on prescription bottles before you throw them out. Don't share your health plan information with anyone who offers free health services or products.

c. Away from home:

	AWAY	
	Paper	**Digital**
5 min	Letter*	Cloud Storage*
5 hours	Correspondence	Cloud Storage
5 days	(Re)Organization efforts, P.O. Box, Storage Unit	Backups, P.O. Box storage, Storage Unit
5 months	Mail-in archives	Website, Blog
5 years+	Review storage keys, locations, combination locks, Family Reunion books & material	Review passwords, digital keys, privacy policies, Family Reunion DVD & material

i. In-store photo service: Walmart, Costco, Walgreens
ii. Mail-in Photo service: http://www.imemories.com/, http://www.scanmyphotos.com/, http://www.fotobridge.com/
iii. How to modernize slides: http://www.komando.com/tips/368756/how-to-modernize-your-old-photos-and-slides?utm_medium=nl&utm_source=totd&utm_content=2016-08-19-article-b
iv. Digitizing Photos: http://www.pcworld.com/article/2000199/the-best-and-worst-services-for-digitizing-your-photos.html
v. BYU FHL Equipment: http://guides.lib.byu.edu/c.php?g=216346&p=1428420
vi. Limit what you carry. Take only documents you need when you go out.
vii. Ask why people request information from you.
viii. If you won't be home for several days, request a **vacation hold** on your mail.
ix. Be Alert to Impersonators

d. Online Safety
i. Sensitive websites: Look for "HTTPS" or the Lock image
ii. Don't Overshare on Social Networking Sites
iii. Keep Passwords (Passphrases) Private
iv. Passwords:
v. http://www.komando.com/columns/371600/new-password-rules-make-them-easy-to-remember-and-more-secure?utm_medium=nl&utm_source=totd&utm_content=2017-02-05-video-c
vi. Password Help: https://howsecureismypassword.net/, https://password.kaspersky.com/, https://www.lastpass.com/
vii. Biometrics slowly being adopted (fingerprint scanner, etc)

e. Protecting Infromation
i. THEFT: After using copies of documents, SHRED THEM.
ii. FIRE: fireproof safe or envelopes
iii. WATER: waterproof containers
iv. Preserve your work: http://www.genealogy.com/articles/research/67_donna.html

f. Redundancy vs.Backups
i. REDUNDANT: Multiple copies of your CURRENT or LIVE data
ii. BACKUP: one or more VERSIONS of data you own (historical, etc)
iii. Storage Space – how much do you need?
iv. How QUICKLY will you need to get your data?
v. Is the service reliable for your needs?
vi. Is it EASY to UNDERSTAND how to put files in, and get files out?
vii. SSD Failures: Not all thumbdrives are equal. Not all harddrives are equal
1. DEPENDS on frequency of use, temperature, and air quality
2. Within four years, more than 20% of flash drives were found to have uncorrectable errors.
3. http://www.komando.com/happening-now/349753/your-ssd-can-be-putting-your-treasured-photos-and-files-at-risk

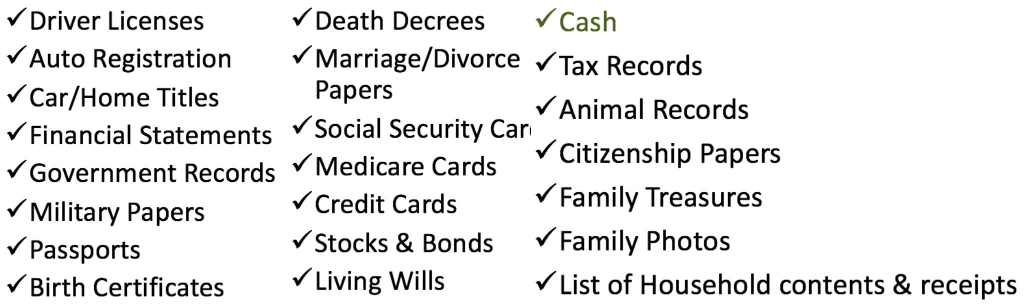
g. Protecting Family History Data
i. Preserve your family history data (text, photo, video, tree):

        - 1. Ancestry.com: Family History
        - 2. FamilySearch.org: Family History
        - 3. FindMyPast.com: Family History
        - 4. MyHeritage.com: Family History
    - ii. Other Family History resources:
        - 1. 23andMe.com: DNA testing
        - 2. ChroniclingAmerica.loc.gov: Part of Library of Congress, contains digitized newspapers; not for storing personal data
        - 3. BillionGraves.com & FindAGrave.com: Cemetery Records; You can add some info about an ancestor but it's limited.
        - 4. Fold3.com: Military Records site owned by Ancestry.com
    - iii. **Use more than one website or storage solution to store your online Family History data!** This keeps your files safe from computer crashes, theft and local disasters. The files are encrypted on your computer and sent over an encrypted connection, so hackers don't have a shot of getting your sensitive financial information.

- 3. Digital Organizational Behavior
    - a. Cloud Backup
        - i. Carbonite.com
        - ii. Acronis.com
        - iii. Backblaze.com
        - iv. Crashplan.com
        - v. SOSOnlineBackup.com
        - vi. www.SugarSync.com
        - vii. Mozy.com
        - viii. OpenDrive.com
        - ix. IDrive.com
        - x. SpiderOak.com
        - xi. Backup.com (Norton)
        - xii. DataDepositBox.com
        - xiii. MegaBackup.com (example of a service that uses another company: Amazon)
        - xiv. Article: "Best Online Backup Services of 2017" http://www.pcmag.com/article2/0,2817,2288745,00.asp
        - xv. Article: "24 Online Backup Services Reviewed" https://www.lifewire.com/online-backup-services-reviewed-2624712
    - b. Mobile Device Backup
        - i. Android
            - 1. Android Backup Service
                - a. **add a backup account**. Here is how to do that:
                - b. Open your gadget's Settings app
                - c. Under "Personal," tap **Backup & reset**
                - d. Tap **Backup account >> Add account**
                - e. Confirm your gadget's PIN, pattern or password
            - 2. AirMore (file transfer)
                - a. https://play.google.com/store/apps/details?id=com.airmore
        - ii. iOS (iPhone, iPad)
            - 1. iCloud
                - a. http://www.apple.com/icloud/
            - 2. AirDrop
                - a. Apple AirDrop is a built-in app that lets you seamlessly move files back and forth between nearby desktop Macs and iOS gadgets like iPad, iPhone or iPod touch.
                - b. To enable AirDrop on an iPhone, iPad, or iPod touch, swipe up on the Home screen to access the Control Panel. From here, you can set AirDrop to receive from Contacts Only, Everyone, or turn it Off.
        - iii. Article: "Easiest Way to Backup your Smartphone" http://www.komando.com/tips/383758/easiest-way-to-backup-your-smartphone/3
    - c. Reverse Cloud Example – Backup your Gmail
        - i. http://www.upsafe.com/free-gmail-backup/
    - d. Cloud Storage Comparisons
        - i. DropBox.com
        - ii. Google.com/drive
        - iii. Onedrive.live.com
        - iv. iCloud.com
        - v. Box.com
        - vi. Amazon.com/clouddrive
        - vii. Nextcloud.com
        - viii. pCloud.com
        - ix. Zoolz.com
        - x. LiveDrive.com

- e. Is the Cloud Safe?
  - i. PROS:
    - 1. Usability: I can drag/drop, etc.
    - 2. Bandwidth: I can share a link, and not just email files to others
    - 3. Accessibility: Where there is Internet, there is my data
    - 4. Disaster Recovery: Backups are done at a remote facility
    - 5. Cost Savings: I benefit from bulk hardware/software costs; pay-as-you-go
  - ii. CONS:
    - 1. Responsibility: What level of trust can you place in another company? Perhaps they allow governments to look at their data.
    - 2. Bandwidth: Do I get charged for metered Internet activity (ie. Will using this service incur high data costs)? Costs can be hard to predict.
    - 3. Accessibility: If I don't pay the bill, or I don't have Internet access, I don't get to access my data! Also, there may be outages.
    - 4. Data Security: Is my personal data on the same servers as others? Will they be able to access (or hack into) my data?
    - 5. Software: Do I need to download an app or program on every device I use, to access my data? You might be locked-in to their technology.
  - iii. Mitigate Risks of Cloud Storage:
    - 1. **Encrypt your data** before storing it elsewhere – so they can't see your data, they will just store it
    - 2. Use Multiple Storage providers
- f. Questions to Ask Cloud Service Providers:
  - i. How long have you been in business?
  - ii. Where will my information be stored? For how long?
  - iii. Do you use your own servers? Or outsource to another company?
  - iv. What is your privacy policy?
  - v. What type of security does your cloud have?
  - vi. What happens if you go out of business? Or I cancel my account?
  - vii. What are your costs / fees?

4. Prioritize with a Plan
   - a. Home Readiness Checklist



✓Driver Licenses
✓Auto Registration
✓Car/Home Titles
✓Financial Statements
✓Government Records
✓Military Papers
✓Passports
✓Birth Certificates
✓Death Decrees
✓Marriage/Divorce Papers
✓Social Security Car
✓Medicare Cards
✓Credit Cards
✓Stocks & Bonds
✓Living Wills
✓Cash
✓Tax Records
✓Animal Records
✓Citizenship Papers
✓Family Treasures
✓Family Photos
✓List of Household contents & receipts

   - b. Home Emergency Checklist
     - i. If a disaster happened, could you recover:
       - 1. Financially?
       - 2. Emotionally?
       - 3. Physically?
     - ii. Create a "room-by-room" Emergency Plan
       - 1. Ideas: https://www.pinterest.com/explore/emergency-binder/
   - c. Preserving Photos:
     - i. Scanning: http://genealogysstar.blogspot.com/2014/05/free-scanning-service-offered-at-family.html
     - ii. Digital Conversion Services: https://www.larsendigital.com/services.html
   - d. Cut Your Losses
     - i. Prepare for time constraints or other resource restrictions:
       - 1. Can't check out a book?
       - 2. Can't Photocopy or Photograph Material?
       - 3. Can't stay overnight!

e. Research Abroad Checklist

✓Thumbdrive

✓Cloud Account Credentials

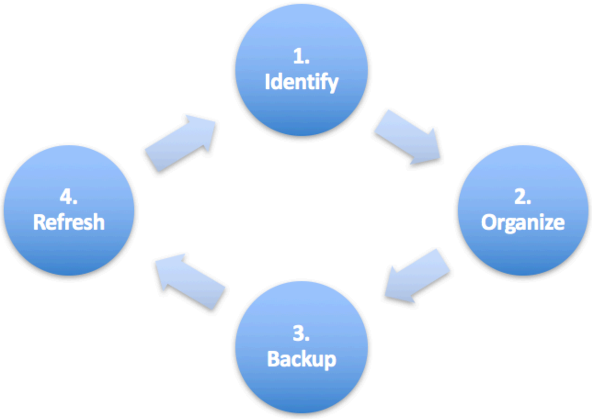
✓Pen & Paper

✓Backup Power (charger)

✓Mobile Device(s)

- Audio, Video Recording
- Record-keeping

5. The Opportunity Cost of Preparedness
   a. "Opportunity Cost": *the loss of potential gain from other alternatives when one alternative is chosen*
      i. The choice of one path precludes all others…
   b. What would we lose by NOT doing this Family History work?
   c. Discipline; Take the TIME to do these things, however inconvenient they may be:



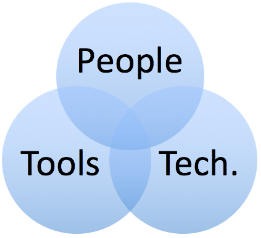
      i. IDENTIFY the items you need to safeguard
      ii. ORGANIZE those items in terms of priority, type, location, etc
      iii. BACKUP items physically, electronically, and in different locations
      iv. REFRESH your backups on a regular basis; verify that they are still safe; REPEAT
   d. On Guard
      i. SCAMS: "a dishonest scheme; a fraud; swindle."
         1. https://www.usa.gov/scams-and-frauds
         2. https://www.consumer.ftc.gov/scam-alerts
         3. http://www.bbb.org/council/bbb-scam-stopper/top-scams/
      ii. RANSOMWARE: "malicious software designed to block access to data until a sum of money is paid."
         1. https://heimdalsecurity.com/blog/what-is-ransomware-protection/
         2. http://www.watchguard.com/wgrd-solutions/security-threats/ransomware
         3. The FBI recently gave recommendations on how to avoid ransomware attacks:
            a. Download only trusted software - Make sure the software you download comes from trusted sites. In this instance, the malicious app actually was found in the Google Play Store. However, this is very rare and the Play Store is the most trusted place for Android users to find safe apps.
            b. Back up data regularly - this could be the best way to recover your critical data if you are infected.
            c. Make sure your backups are secure - do not connect your backups to computers or networks that they are backing up.
            d. Never open risky links in emails - don't open attachments from unsolicited emails.
            e. Have strong security software - This will help prevent the installation of ransomware on your gadget.
      iii. MALWARE: "software intended to damage or disable computers and computer systems."

        1. http://www.watchguard.com/wgrd-products/security-services/advanced-malware-protection
        2. http://www.top10bestantivirus.com/best-malware-protection
    - iv. PHISHING: “to entice individuals to reveal personal information in a fraudulent manner, for fraudulent purposes”
        1. https://www.bbb.org/scamtracker/us/

6. Staying Ten Steps ahead of the Time Traveling Bandits
    - a. References:
      https://www.theguardian.com/technology/2013/sep/16/10-ways-keep-personal-data-safe
      https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure

        1. File Storage and Handling
            - a. Safe, Envelopes, Safety Deposit Box, Organization; Make Copies
            - b. Use Security Software
        2. Web Browsing
            - a. Ad Blocker, HTTPS, Lock, Incognito Mode (Chrome browser)
        3. Search Engines (Incognito)
            - a. Clear your cache & browsing history; try DuckDuckGo.com
            - b. If you want to be private and anonymous online, try: https://tails.boum.org/getting_started/index.en.html
        4. Email Details
            - a. Many “free” email providers scan email contents; Use REPLY carefully
        5. Beyond the Password
            - a. Try a “passphrase” approach; create a phrase, then append (or prepend) unique letters & numbers relevant to the context of each password’s purpose.
            - b. Article on Security Breaches: https://www.pluralsight.com/blog/career/cyber-security-tips-troy-hunt
        6. Encryption Considerations
            - a. Encrypt data when applicable; Try “BitLocker” or “GPG for Mail” or “FileVault” or even encrypted email such as “Enigmail”
        7. Social Networking
            - a. Be very careful whenever you give out personal information, such as Date of Birth, etc. Also, be cautious when using social media sites on PUBLIC computers. This includes any site that requires a password, when using a PUBLIC computer.
        8. Cloud Services
            - a. Take the time to research the aspects of Cloud Services that are important to you: quick access, low cost, replication, privacy, encryption, etc.
        9. WiFi Walls
            - a. Set limits to your discoverability, for your protection. This includes WiFi and Bluetooth, as your activity may be susceptible to prying eyes or theft.
        10. Location is Key
            - a. Many apps require or request your location; ensure that you aren’t over-extending your trust by turning off location when it is not necessary.

7. Security is a Process, not a Product
    - a. There are three roots to security challenges:



    - b. “Security is a Process, not a Product; Security products will not save you.” – Bruce Schneier
    - c. Keeping history safe is a continual effort, and not a destination
    - d. If we can consistently review our roots (data), we have a better chance in keeping ourselves, and our posterity safe!

“Your ancestors are rooting for you.” — Eleanor Brownn