HOW TO FOLLOW THE MACHINE

A Field Guide for Open-Source Investigators

Troy Barile

thefalloutwithtbs.substack.com

grifter-nation.com · grifter-nation.help · followthefiles.com

A NOTE ON PRICE

The suggested price for this workbook is $10. That amount directly supports the ongoing investigation documented in The Machine series at thefalloutwithtbs.substack.com. If you can pay it, please do. If you cannot pay anything at all, use it well and share it with anyone that may also benefit from this guide. The work matters way more than the money.

LEGAL DISCLAIMER

This workbook is a guide to using publicly available information and open-source tools. Nothing in it constitutes legal advice. Nothing in it authorizes or encourages illegal activity, harassment, unauthorized access to private information, or the publication of unverified claims. The author is not a lawyer. If you receive legal threats in connection with your research, consult an attorney. The tools, databases, and methods described here are intended for lawful, responsible, and ethical use only.

COMPANION WEBSITE

This workbook has a living companion at followthefiles.com. Every tool, database, and URL referenced in these pages is maintained and updated there. Links change, databases update, and platforms evolve. The workbook gives you the foundation and the website keeps it current. Use both.

For the survivors who kept talking when no one was listening.

And for everyone who decided to look.

A NOTE BEFORE YOU BEGIN

I built this because people kept asking me how.

Every week since The Machine series started, someone finds me and asks the same question in different words. How do you find this stuff? Where do you look? How do you know what's real? How do you document it in a way that actually holds up? How do you do this without getting yourself destroyed in the process?

I'm not a trained journalist. I don't have a newsroom behind me or a legal department or institutional protection. What I have is a method that I developed by doing the work — by pulling court filings and corporate records and social media archives and federal documents until I understood how they connect to each other and how to present what they show without overstating it.

This workbook is that method, written down so you can use it.

Everything in here uses tools that are free or low-cost and publicly accessible to anyone with an internet connection. There is no inside access required, press credentials, or special database subscriptions that cost thousands of dollars a year. The Epstein files are public, the court records are public, Companies House is public, ProPublica's Nonprofit Explorer is public, and social media is public. Most of what I have published in this series came from sources that you could pull up in your browser right now if you knew where to look and what to do with what you found.

That's what this teaches you.

It will not make you an instant investigator. Nothing does that. What it will do is give you the foundation — the habits, the tools, the documentation standards, and the understanding of what you're actually looking at when you find something — that separates a person who can produce credible, publishable findings from a person who has a lot of tabs open and a strong opinion.

The difference matters. The people running active operations against Epstein survivors count on the people paying attention being disorganized, undisciplined, and easy to discredit. **This workbook is how you make yourself harder to dismiss.**

Do the work carefully, verify everything, label allegations as allegations and confirmed facts as confirmed facts, archive everything before you publish anything, and use followthefiles.com alongside this book — that's where the living version of every tool, database, and resource lives, updated as things change.

Let's get into it.

— Troy Barile

thefalloutwithtbs.substack.com · grifter-nation.com

FOREWORD

Why This Exists

The files are out and so is the machine that's still running.

In January 2026, the Department of Justice released over three million documents from the Epstein investigation. Three million pages. One hundred and eighty thousand images. Two thousand videos. The biggest document dump connected to a single criminal case in modern American history.

And most of the public conversation since then has been about names.

Which celebrities are in the contact book. Which politicians appear on the flight logs. Who attended which dinner. Whether someone shook the man's hand at a party in 1998. That conversation is legitimate — I am not dismissing it because accountability for the people who enabled Epstein and Maxwell is the whole point. But there is another conversation that is barely happening, and it is the one that I have spent the better part of a year trying to make people see.

The machine that protected this network while it was operating, and that is actively working to protect it now that Maxwell is convicted and the files are public, is not in those documents. It is on X, Substack, in the comment sections of articles about Virginia Giuffre, and even on Telegram channels with seventy thousand subscribers. It is named — some of its operators explicitly by name — in federal witness harassment complaints released as part of the same file dump that everyone is reading for celebrity names.

The people running it are not hiding. They have verified checkmarks, do podcasts, take photos at Mar-a-Lago, have book deals, call themselves journalists, and they even describe Ghislaine Maxwell's conviction as an American disgrace. They post KARMA over photographs of dying survivors and are named in the same DOJ document as Maxwell herself. Due to the fact that people paying attention are largely focused on what's in the files rather than on what is happening right now, these operations run with almost no scrutiny.

That is the gap this workbook exists to close.

I am not asking you to take my word for any of this. The Machine series at thefalloutwithtbs.substack.com is, as of this publishing, twenty-two parts of sourced, documented, named findings about specific people doing specific things. What I am asking you to do is learn how to look for yourself — because the more people who know how to do this work, the harder it is for the machine to keep running.

This is not a theoretical exercise. The things this workbook teaches you to find are the things that belong in front of Congress, in front of the FBI, and in front of the public. The congressional contact tool at grifter-nation.com exists because documented findings with proper sourcing are the only thing that creates the pressure for subpoena power. You are not just learning to research but also how to produce the kind of evidence that can actually do something.

Start here. Take your time. Do it right.

PART ONE

Before You Start

Mindset, protection, and the habits that separate credible investigators from people who just have a lot of tabs open.

CHAPTER 1

The Mindset of an Open-Source Investigator

One thing separates an investigator from someone with a theory.

That one thing is the chain of evidence. Every claim has a source and every source is named. Allegations are labeled as allegations. Verified facts are labeled as verified facts. The moment you publish something you cannot source, you have handed the people you are investigating a weapon they will use against you — and against the survivors whose accounts you are trying to amplify.

This is not just an ethical standard but a strategic one. The machine documented in this series has lawyers, people whose full-time job is to find the thing you said that you cannot prove and use it to discredit everything else, and the only way to take that weapon away from them is to not give it to them in the first place.

The difference between a lead and a fact

A **lead** is something that points you somewhere. A document that names a person, a post that references a company, or a connection you noticed between two accounts. A lead is not publishable. It is the beginning of research, not the end of it.

A **fact** is something you have verified from a named source that you can cite. A court filing at a specific docket number, a Companies House entry with a specific company number, and a social media post archived at a specific URL with a specific date. A fact is publishable. A lead is not.

Everything in your investigation lives in one of three categories until it is ready to publish. Write these down and use them every time.

- **CONFIRMED** — Verified from a named, citable public source. This is what you publish.
- **ALLEGED / CLAIMED** — Stated in a court filing, a victim statement, or by a named individual. Publishable only when clearly labeled as such.
- **UNVERIFIED** — You found it but cannot source it. Not publishable. Keep researching or cut it.

Why proximity is not guilt — and why it still matters

Being named in the same document as Maxwell is not a conviction. Vacationing with someone connected to Epstein is not evidence of trafficking. Liking a post from a person under investigation is not proof of coordination. These are documented facts that establish proximity. What they mean is a question the reader answers — and your job is to give the reader the documented facts, label them accurately, and let them draw conclusions rather than drawing the conclusions for them and presenting them as fact.

This protects you legally and makes your work more credible. The reader who feels like they reached a conclusion themselves is more convinced than the reader who feels like they were told what to think.

Confirmation bias is the enemy

You will have a theory when you start. That theory will feel increasingly correct the more you research, because research surfaces connections and connections feel like confirmation. **The discipline is to actively look for evidence that your theory is wrong.** If you cannot find it, the theory gets stronger but, if you find do, you must deal with it — either integrate it into a more complex understanding or revise the theory.

The investigators who get things wrong and embarrass themselves — and there are many in this space — are almost always people who decided what was true and then went looking for evidence to support it rather than going where the evidence led.

The ethical lines

- **Do** not publish home addresses of private individuals. If a subject's address is in a court filing or corporate record, you may reference that it exists and what it shows without publishing the street address.
- **Do** not publish information about minors, period. Even if it appears in public records.
- **Do** not contact survivors unsolicited to demand information. If you have documented findings relevant to their situation, reach out through an intermediary if possible and make clear they are under no obligation.
- **Label** everything. If you are not certain it is confirmed, say so. If it is an allegation from a court filing, say that. If it is a claim by a named individual that you cannot independently verify, say that.
- **Give** subjects the opportunity to respond before you publish. Document that you contacted them and what they said, or that you contacted them and received no response. This is not a legal requirement in all jurisdictions but it is a practice that strengthens your work and makes you harder to attack.

WORKSHEET 1.1

My Investigation Standards

Write your own rules before you begin any investigation. These are yours. If you break them, you only have yourself to answer to — but you will answer to yourself.

My sourcing standard (what it takes for me to call something confirmed):

My ethical line on publishing personal information:

My rule on publishing unverified material:

What I will do before I publish anything about a named individual:

What I will do if I receive a legal threat:

CHAPTER 2

Protecting Yourself First

You cannot investigate people with resources and lawyers without thinking about your own exposure.

This is not paranoia, it is preparation. The people documented in The Machine series have lawyers who send cease-and-desist letters. They have supporters who dox journalists, post LCSW provider records of co-investigators' spouses, report Instagram and Substack accounts, and threaten lawsuits they never file because the threat alone is enough to make some people stop.

None of this means you should be afraid but you should be prepared. Preparation is what lets you keep working when the pressure comes.

Device and browser basics

- **Use** a separate browser profile for research. Do not mix your personal browsing with your investigation browsing.
- **A** VPN is useful for general privacy but is not a substitute for secure practices. A good free option is ProtonVPN. Paid options like Mullvad are stronger. You do not need this for basic public records research but it is good practice for anything sensitive.
- **Do** not log into personal accounts (Google, Facebook, Instagram) while doing research you want to keep private. Logged-in browsing is tracked and associated with your identity.
- **Use** Firefox or Brave rather than Chrome for research. Both have better default privacy settings.
- **uBlock** Origin is a free browser extension that blocks trackers. Install it.

Archiving before you publish

The single most important protective habit is this: archive everything before you publish anything. Things disappear, posts get deleted, accounts get suspended, court filings get sealed, and the person you are investigating will sometimes scrub their digital footprint the moment your piece goes live. If you archived before publishing, you have the record. If you did not, you have nothing.

Archive.org (the Wayback Machine) and Archive.today are the two tools you need. Both are free and both create a timestamped, URL-referenced snapshot of a webpage that you can cite.

What to do when someone threatens to sue you

The first thing: do not panic and do not delete anything. Deleting content after receiving a legal threat can be used against you. **The second thing**: save the threat itself — screenshot it, save the email, document the date. **The third thing**: consult an attorney before responding. In the United States, the Reporters Committee for Freedom of the Press (rcfp.org) operates a legal defense hotline for journalists and independent reporters. The ACLU also has resources. Do not respond to legal threats on your own without at least reading RCFP's guidance.

Most threats in this space are not followed by actual lawsuits. They are designed to make you stop. The documented record of receiving a threat and continuing to publish responsibly is itself a form of protection — it shows you took the threat seriously, evaluated it, and determined your reporting was sound.

WORKSHEET 2.1

My Research Setup Checklist

Complete this before starting any investigation. Check each item when it is in place.

- ☐ Dedicated research browser profile set up
- ☐ VPN installed (ProtonVPN free / Mullvad paid)
- ☐ uBlock Origin installed
- ☐ Archive.org account created (free)
- ☐ Archive.today bookmarked
- ☐ Secure note or folder system for saving findings
- ☐ Cloud backup system in place for archived files
- ☐ RCFP hotline number saved: 1-800-336-4243
- ☐ Personal accounts NOT logged in on research browser
- ☐ Screenshot tool that captures full URL and timestamp configured

WORKSHEET 2.2

Legal Threat Response Card

Fill this out before you publish anything. Having the information ready removes panic from the equation.

My attorney's name and contact:

RCFP Legal Defense Hotline: 1-800-336-4243 (pre-filled — confirm this is current at rcfp.org)

My archive storage location (where I keep screenshots and archived URLs):

My co-investigator's contact in case I go offline:

- ☐ If I receive a threat: DO NOT DELETE ANYTHING
- ☐ Screenshot and save the threat with date and time
- ☐ Do not respond without consulting an attorney or RCFP
- ☐ Document that I continued publishing responsibly
- ☐ Contact followthefiles.com community for peer support

CHAPTER 3

How to Archive Everything

Courts have asked for archives that no longer exist. Don't be the person who has nothing to show.

Archiving is not optional and is the foundation of everything else. A post you screenshot but did not archive can be claimed to be altered but an archive with a URL and a timestamp cannot. This is the difference between "I saw it" and "here is the record that it existed."

The two tools you need

- **Archive.org / Wayback Machine (web.archive.org)** — Go to the site, paste the URL you want to archive, click Save. It creates a snapshot at a specific date and time and gives you a permanent URL you can cite. Free. Accepted in court.
- **Archive.Today (archive.ph / archive.is)** — Faster, better for social media posts, captures dynamic content that Wayback sometimes misses. Paste the URL, click Archive. Free.
- **Use** both for anything you plan to publish. One as backup to the other.

What to capture in every screenshot

A screenshot without context is not a citation. Every screenshot you save should show all of the following, visible in the frame:

- **The** full URL in the browser address bar
- **The** date and time (if the platform shows it — if not, note it separately)
- **The** username or account name of the person who posted
- **The** follower count or account verification status if visible
- **Enough** surrounding context that the post cannot be claimed to be taken out of context

File naming that makes sense later

Six months from now you will not remember what IMG_4892.png contains. Before you save any screenshot or archive, rename it. A system that works:

- **SUBJECT-PLATFORM-DATE-DESCRIPTION.png**
- **Example**: Tonks-X-20241102-DuPont-post.png

- **Example**: Ziegler-WhatsApp-202x-Wexner-message.png

Keep a master folder per subject. Inside it: a Documents subfolder, a Screenshots subfolder, an Archives subfolder (text files with archive URLs), and a Notes document.

WORKSHEET 3.1

Archive Log Template

Make a copy of this for every investigation. A running record of everything you archive.

Date	Platform / URL	Content Description	Archive Link (archive.today or Wayback)	File Saved Locally

PART TWO

The Public Record

Court filings, corporate registries, nonprofit 990s, government databases, and the Epstein files specifically. Everything starts here.

CHAPTER 4

Court Records

Federal and state court systems are public. Most people never look.

Court filings are the most authoritative public record you will ever use. They are statements made under oath, by attorneys and parties who face professional and legal consequences for lying. When a judge calls a motion "totally devoid of merit" and awards attorney fees, that is a documented, citable fact. When a plaintiff alleges in a sworn complaint that someone impersonated a donor to extract confidential information and then published their home address, that is a documented, citable allegation. The distinction is important and both belong in your work.

PACER — Federal Courts

PACER (Public Access to Court Electronic Records) is the federal government's public court document system. It covers all federal district courts, circuit courts of appeal, and the Supreme Court. Every federal civil and criminal case is there.

- **Create** a free account at pacer.gov
- **Cost**: $0.10 per page, with a quarterly waiver for accounts that spend under $30. Most searches cost very little.
- **Search** by party name, case number, or attorney name
- **What** you find: complaints, motions, orders, judgments, dockets. The docket is the index of everything filed in a case.

CourtListener — The Free Alternative

CourtListener (courtlistener.com) is operated by the Free Law Project, a nonprofit. It mirrors a significant portion of PACER for free, plus it contains the full text of opinions going back decades. Search by party name and you will often find what you need without touching PACER. When you need the actual filings rather than just opinions, PACER is where you go.

State Courts

Every state has its own court system and its own public access portal. Uniformity of access varies widely — some states have excellent free online search tools, some require you to go in person. CourtReference.com maintains a state-by-state directory of court search portals. For the UK, the

Court of Justice system has public search tools and Companies House is where corporate litigation often surfaces.

How to read a docket

The docket is the running index of everything filed in a case. It shows you the case number, the parties, their attorneys, and every filing in chronological order with a date. Reading a docket tells you: when was this filed, what stage is it in, what motions have been made and ruled on, and what is the current status. You do not need to read every filing — start with the complaint (the original filing that explains what happened) and the most recent order (what the judge last decided).

Criminal vs. Civil

- **Civil** cases are disputes between parties — lawsuits for damages, injunctions, contract disputes. The standard of proof is "preponderance of the evidence" (more likely than not).
- **Criminal** cases are brought by the government against a defendant. The standard of proof is "beyond a reasonable doubt." A criminal conviction is a stronger factual foundation than a civil judgment.
- **A** civil dismissal does not mean someone is innocent. It may mean the plaintiff settled, ran out of money, or the court found procedural problems. Read the dismissal order before drawing conclusions.

WORKSHEET 4.1

Court Record Tracker

Subject Name	Jurisdiction	Case Number	Case Type	Status	Key Findings	Archive Link

WORKSHEET 4.2

Docket Reading Guide

Use this to break down any docket you are analyzing.

Case name and number:

Court / Jurisdiction:

Date filed:

Plaintiff(s):

Defendant(s):

Plaintiff's attorney(s):

Defendant's attorney(s):

What the complaint alleges (summary):

Key motions filed and outcomes:

Current status of the case:

Key language from judicial orders worth quoting (with page/line references):

CHAPTER 5

Corporate and Business Records

The people running the machine all have corporate footprints. This is where you find them.

A corporate filing tells you things a social media profile never will. Who co-founded something with whom, what address they used, what they said the company was for, who the shareholders are, and whether they dissolved the company in a hurry after scrutiny arrived. **The UK Companies House filing that showed Sarah Ferguson and Antonia Marshall as co-directors on the same registered company was a fact that fundamentally changed the documented relationship between those two people**. That document is free and publicly available to anyone who looks.

UK Companies House

Companies House (www.gov.uk/government/organisations/companies-house) is the UK government's official registry for all UK limited companies. Every company must file: its directors (with date of birth month and year), its shareholders, its registered address, its SIC (business activity) code, and annual accounts. All of it is free to search and download.

- **Search** by company name or officer name
- **The** officer appointments page shows every company a person has ever been a director of, active and dissolved
- **The** persons with significant control (PSC) page shows shareholders
- **The** filing history page shows every document ever submitted — download accounts and annual returns for the full record
- **Dissolved** companies still have their full filing history available

WHAT TO LOOK FOR IN COMPANIES HOUSE

Co-directors who share correspondence addresses with people under investigation. Registered addresses that are shell agent addresses (used by thousands of companies with no physical office). SIC codes that don't match the claimed purpose. Companies dissolved suddenly after public scrutiny. Cross-references between subjects — if two people under investigation are co-directors of the same company, that is a documented formal relationship.

US State Business Registries

Every US state maintains a business registry. Quality of free access varies significantly. The most important states for this investigation are Wyoming and Delaware — both are notoriously permissive incorporation jurisdictions used for shell companies and holding entities.

- **Wyoming** SOS: wyobiz.wyo.gov
- **Delaware** Division of Corporations: icis.corp.delaware.gov
- **Nevada** SOS: esos.nv.gov
- **Most** other states: search "[state] secretary of state business search"

How to read a corporate filing

- **SIC Code** — Standard Industrial Classification. Describes what the company does. "Other business support service activities n.e.c." means they filed a placeholder code that tells you nothing. That itself is worth noting.
- **Registered Agent** — The address where legal documents are served. When multiple companies share the same registered agent at the same address, it often indicates a professional shell service rather than a genuine business operation.
- **Correspondence Address vs. Registered Office** — In UK filings, these can be different. A correspondence address at a private residence is notable. A correspondence address at Royal Lodge, Windsor is very notable.

WORKSHEET 5.1

Corporate Entity Tracker

Entity Name	Jurisdiction / Number	Inc. Date	Status	Directors	Registered Agent	Key Findings

WORKSHEET 5.2

Corporate Network Map

Draw the connections between entities and individuals. Each circle is a person or company. Each line is a documented connection. Label each line with the type of connection (co-director, shareholder, shared address, etc.) and its source.

CHAPTER 6

Tax Records and Nonprofit Filings

Nonprofits file 990s. 990s are public. They show who is getting paid, from where, and whether the numbers match the story.

A 990 is the annual tax return filed by every US nonprofit organization with the IRS. It is public. It shows total revenue, total expenses, compensation paid to officers and key employees, a list of board members, a description of the organization's activities, and whether revenue comes from named or anonymous sources. An organization that takes in $612,000 in a single year with 100% of donations from anonymous sources and negative net assets in the following year has a documented financial story that is worth understanding.

ProPublica Nonprofit Explorer

nonprofit.propublica.org is the easiest way to access 990s for free. Search by organization name or EIN (Employer Identification Number). You can download the full 990 as a PDF or view key fields in their database. The data goes back to 2001 for most organizations.

What to look for in a 990

- **Revenue sources** — Is revenue from program services (they actually do something), government grants, or contributions? What percentage is from anonymous individual donors? A 990 that shows 100% of revenue as anonymous individual contributions for multiple consecutive years with no named institutional funders is unusual.
- **Officer compensation** — What are named individuals being paid? Compare to total revenue and stated mission.
- **Net assets** — Is the organization accumulating resources or running at a deficit? Negative net assets mean the organization owes more than it has.
- **Related organizations** — Does the 990 disclose relationships with other entities? This can reveal a corporate network you would not otherwise see.
- **Schedule O** — The narrative section where organizations explain their activities. Read this carefully. Vague language here often indicates a vague actual purpose.

WORKSHEET 6.1

Nonprofit 990 Analysis Template

Organization name and EIN:

Year of filing:

990 URL / ProPublica link:

Year	Total Revenue	Anon Donations %	Officer Compensation	Net Assets	Key Notes

Board members named:

Stated mission vs. apparent actual activity (your assessment):

Red flags identified:

CHAPTER 7

Government Databases

The government publishes more about people than most people realize. Most of it is free.

Between PACER, BOP, the FAA registry, the FEC, and professional license databases, a significant portion of a person's institutional footprint is in public government databases right now. The skill is knowing which database to check and how to read what it returns.

Federal Inmate Locator

bop.gov/inmateloc — The Federal Bureau of Prisons maintains a public inmate locator. Search by name or Register Number. Shows current facility, projected release date, offense, and sentence. This is how you confirm that someone claiming to be a federal inmate is actually a federal inmate — and how you verify BOP Register numbers cited in federal documents.

Federal Election Commission

fec.gov — Every contribution to a federal PAC, Super PAC, or campaign committee above $200 is disclosed publicly. Search by donor name, organization name, or recipient. If someone claims not to be connected to a political operation but their name appears in FEC filings as a donor to a PAC that has demonstrable connections to the network you are investigating, that is a documented fact.

FAA Aircraft Registry

registry.faa.gov — The FAA maintains a public registry of all registered aircraft in the United States. Search by owner name or tail number (N-number). This is how flight log analysis begins — you identify the aircraft, confirm its ownership through the registry, and cross-reference with ownership records to establish who controlled the aircraft at the time of a documented flight.

Professional License Databases

Every state maintains public records of professional licenses — attorneys, medical professionals, real estate agents, private investigators, social workers, therapists. These databases confirm that a license exists, show any disciplinary actions, and in some states show an address or contact. An Illinois private investigator license number like 9684 is a verifiable public record that tells you the person holds an active law enforcement-adjacent credential in that state.

FOIA — Freedom of Information Act

The Freedom of Information Act gives you the right to request federal government records. Muckrock.com is the best tool for filing and tracking FOIA requests — it manages the submission, tracks deadlines, and publishes completed requests so other researchers can see them. FOIA requests can take months or years and are frequently denied or heavily redacted. File them anyway. The paper trail matters and sometimes what comes back is significant.

WORKSHEET 7.1

Government Database Master Checklist

For each investigation, run through this list. Check the box when searched, note the result.

Database	URL	Date Searched	Search Term Used	Result / Notes

WORKSHEET 7.2

FOIA Request Tracker

Agency	Request Date	Subject / Description	Tracking Number	Response Due	Response Received	Appeal Filed

CHAPTER 8

The Epstein Files Specifically

Three million documents. Here is how to navigate them.

In January 2026, the DOJ released over three million pages of documents, 180,000 images, and 2,000 videos related to the Epstein investigation. Most people who are paying attention to these files are doing full-text searches for famous names. That is a legitimate use of the archive but the files contain more than contact books and flight logs — they contain victim statements, FBI communications, harassment complaints, and evidence submissions that document what is happening right now, not just what happened in the past.

> **CRITICAL DISTINCTION**
>
> *A name appearing in the Epstein files does not mean that person committed a crime, was a victim, or was involved in trafficking. Names appear for many reasons — as contacts, as people Epstein knew socially, as people referenced in emails without context. Always read the document context, not just the name. Your citation should describe what the document actually says, not just that a name appeared.*

Where to find the files

- **justice.gov/epstein** — The official DOJ repository. Organized by release batch. Not easily searchable by keyword.
- **epstein-data.com** — A community-built archive and search tool. Full-text search across the released documents. The most useful tool for keyword searching.
- **epsteingraph.com** — A relationship mapping tool built from the files. Allows you to see documented connections between named individuals.

EFTA document numbering

Documents released under the Epstein Files Transparency Act use the designation EFTA followed by a number. EFTA01652016 is a specific document. When you cite one, cite it by its full designation, the repository where you found it, and the page number if relevant. "DOJ document EFTA01652016, available at epstein-data.com" is a complete citation.

What the files don't contain

The DOJ stated that its January 30, 2026 release was the final release and that it had met its legal obligations. Critics, including multiple members of Congress, disputed this. Significant redactions remain. Names that congressional members identified in unredacted viewing sessions — like Les Wexner — were later unredacted under pressure but only after months of non-disclosure. The files are extensive but incomplete. Treat them as a partial record, not a definitive one.

How to document a finding from the files

- **Screenshot** the specific page showing the relevant content — with the document number visible
- **Archive** the URL at archive.today
- **Note** the EFTA document number and page number
- **Quote** precisely and label the context — "A victim statement in EFTA01652016 alleges..." not "The Epstein files prove..."
- **Cross**-reference: does the same name appear in other documents? In victim statements? In FBI memos? In flight logs?

WORKSHEET 8.1

Epstein Files Search Log

Search Term	Repository	Date	Documents Found (EFTA#)	Context of Appearance	Key Finding	Archive Link

WORKSHEET 8.2

Subject Profile From the Files

Subject name:

EFTA Document #	Document Type	Page	How Subject Appears	Context	Confirmed/Alleged/Unverified

Cross-references with other subjects in the files:

Summary of documented file record (what it shows, what it does not show):

PART THREE

Social Media & Digital Footprint

Where the machine actually operates. How to document what you find there.

CHAPTER 9

Building a Social Media Profile

Platform by platform — what each one shows, what it hides, and how to document it correctly.

The machine documented in The Machine series does not hide. It operates publicly, on platforms with large audiences, often with verified checkmarks and significant follower counts. The research challenge is not finding it — it is documenting what you find in a way that will hold up when you publish, and organizing it so that connections become visible across platforms rather than buried in individual screenshots.

Platform-by-platform guide

- **X** — Public posts, replies, likes, and follows are visible on most accounts. The advanced search operator is essential (see Chapter 11). Accounts can be suspended but their public posts are often archived by third-party tools. Verified (blue check) status is documented by screenshot.
- **Threads** — Meta's platform. Public posts visible without an account. Growing archive of content from subjects who migrated from Twitter. Good for finding current statements.
- **Instagram** — Public posts visible. Stories disappear after 24 hours — screenshot immediately. Captions, location tags, song choices, and who comments on posts are all documentable. Tagged photos show associations.
- **Telegram** — Public channels are fully accessible without an account. Search by channel name or username. Telegram is where the most unguarded statements often appear because subjects believe their audience is controlled. Archive.today handles Telegram pages reasonably well.
- **Gab** — Fully public. No account required to view. Favored by subjects who have been banned from mainstream platforms. gab.com/[username] — document the profile page and individual posts.
- **Substack** — Public posts visible. Notes and community posts may require an account. Publication About pages document stated mission and background. The publication's archive shows the full history of what was published and when.
- **TikTok** — Public videos visible. Username, follower count, description, and all public videos are documentable. Use a screen recorder for video content since screenshots miss motion.
- **Truth Social** — Requires an account to view most content but the platform has poor content moderation and statements made there are often screenshotted and redistributed. Document the redistribution and the original simultaneously when possible.

How to document a social media post correctly

This is not optional. A screenshot that does not show the username, URL, and date is not a citation. It is an allegation. Every post you document for potential publication needs all of the following:

- ☐ Full URL visible in the browser address bar
- ☐ Account username clearly visible
- ☐ Verification status visible (blue check, or absence of one)
- ☐ Follower count visible if shown on the page
- ☐ Date and time of post (some platforms require you to hover over the timestamp)
- ☐ Full text of the post — do not crop
- ☐ Any media in the post (describe in notes if video)
- ☐ Engagement counts (likes, shares, views) at time of screenshot
- ☐ Archive URL from archive.today or Wayback Machine

WORKSHEET 9.1

Social Media Platform Tracker

One row per platform per subject.

Platform	Username / URL	Verified?	Follower Count	Date Checked	Notable Content	Archived?

WORKSHEET 9.2

Post Documentation Form

Complete one of these for every post you plan to cite in published work.

Platform:

Post URL:

Archive URL:

Account name:

Follower count at time:

Date of post:

Time of post (if shown):

Full text of post (copy exactly — do not paraphrase here):

Images / video description:

Likes at time of screenshot:

Shares / reposts at time:

Context notes (what was this in response to, what was happening around this time):

How I plan to use this (what claim does it support):

Category: CONFIRMED / ALLEGED / UNVERIFIED (circle one and explain):

CHAPTER 10

Mapping a Network Through Social Media

Who talks to whom, who defends whom, and how to make the pattern visible.

Individual posts are data points. A pattern of posts across time and across multiple accounts is evidence. The machine documented in this series did not reveal itself in any single post — it revealed itself through the accumulation of documented interactions: who tagged whom, who amplified whom immediately after a significant event, who rushed to defend whom when scrutiny arrived, who used identical language in posts from different accounts within hours of each other.

What to watch for

- **Immediate amplification** — When Subject A posts something and Subject B reposts it within minutes, consistently, over time, that is a documented pattern of coordination or at minimum a documented close operational relationship.
- **Language replication** — When two different accounts use the same unusual phrase ("extortion and blackmail scheme," "catch and kill") within hours of each other, document both posts with timestamps. The phrase itself is the evidence.
- **Who defends whom unprompted** — When scrutiny arrives on Subject A, who shows up in the comments to defend them? Are those defenders connected to Subject B or Subject C that you are already investigating?
- **Following/follower patterns** — If Subject A and Subject B follow each other despite operating in seemingly different spaces, that is worth noting. It is not proof of anything by itself but it belongs in the file.
- **Tagging patterns** — Who tags whom, in what context, and with what consistency. Tonks tagging Hervey after every significant Epstein development is a documented operational pattern.

Building a visual network map

Draw it. Literally. On paper or in a simple tool like draw.io (free). Put each subject in a circle. Draw a line between any two subjects who have a documented connection. Label every line with the type of connection and its source. When you can see the whole map at once, patterns emerge that are invisible when you are looking at one account at a time.

WORKSHEET 10.1

Network Connection Log

Subject A	Subject B	Platform	Connection Type	Date(s)	Pattern (one-time/recurring)	Archive Link

WORKSHEET 10.2

Network Map Template

Draw your subjects as nodes and their documented connections as labeled lines. Use this space or transfer to a larger format for complex networks.

CHAPTER 11

Platform-Specific Search Techniques

The search operators and methods that surface what a basic search misses.

X Advanced Search

The standard search bar on X searches recent content by keyword. The advanced search (accessible at twitter.com/search-advanced, or via syntax in the search bar) lets you search by date range, by account, and with Boolean operators.

- **from**:username — posts from a specific account
- **to**:username — posts directed at a specific account
- “exact phrase" — posts containing the exact phrase in quotes
- **since**: YYYY-MM-DD until:YYYY-MM-DD — date range
- **Combine** them: from: GeorgeBTonks "Garrett Ziegler" since:2024-01-01

Google Search Operators

- **site:**gab.com "subject name" — searches only Gab
- site:t.me "subject name" — searches Telegram
- “subject name" "specific phrase" — finds both terms together
- “subject name" filetype:pdf — finds PDFs mentioning the name
- **before**: 2024-01-01 after:2022-01-01 — date range for Google results

Finding deleted content

- Wayback Machine (web.archive.org) — enter the URL and browse snapshots by date
- Google Cache — type "cache:URL" in Google — often has recent snapshots
- CachedView (cachedview.nl) — aggregates multiple cache sources
- For deleted tweets: search Wayback Machine for the specific tweet URL if you have it

WORKSHEET 11.1

Search Query Log

Platform	Query / Operator Used	Date	Results Found	Notable Finds	Archive Link

CHAPTER 12

Identity Verification

This is where people make mistakes that cost them credibility. Verify before you publish.

Misidentifying someone is not a recoverable error in this work. The subjects of this investigation have lawyers who are looking for exactly this kind of mistake. An incorrect identification handed them the ability to discredit your entire investigation based on one error. The standard is not "pretty sure." The standard is confirmed from multiple independent sources.

The verification chain

For any individual you plan to name in published work, you want at least two independent, named, citable sources that establish their identity (ideally three). A name that appears in a court filing, with a corresponding Companies House entry with a matching date of birth, and a LinkedIn profile that matches both, is verified. A name that appears in a screenshot and nowhere else is not.

Public identity tools

- **BeenVerified / Spokeo / Whitepages** — Consumer background check tools. Useful for cross-referencing addresses, phone numbers, and associated names. Their data is often incomplete or outdated. Use them to generate leads, not to confirm identity on their own.
- **LinkedIn** — Professional history claims. Not verified by the platform but useful for cross-referencing against public records (does their stated employer match any corporate filing?).
- **Reverse image search** — Google Images (images.google.com), TinEye (tineye.com), and Yandex Images (yandex.com/images). Upload a photo to find other places it appears online. Useful for confirming that a profile photo matches a known individual or for identifying photos used on multiple accounts.
- **Voter registration** — Many states make voter registration data partially public and your state's Secretary of State website is the starting point. Confirms name, address, and sometimes date of birth in public record form.

Documenting aliases

When a subject uses multiple names, aliases need to be documented as carefully as their primary identity. The evidence that a specific alias was used by a specific individual should be traceable: the

conviction records showing David L. DuPont as an alias for George B. Tonks, the sentencing documents listing both names, the BOP registration number that links them — all cited. Never assert an alias without the sourced documentation behind it.

WORKSHEET 12.1

Identity Verification Checklist

Complete before naming any individual in published work.

Subject's confirmed legal name:

- ☐ Court record / government document confirming full name
- ☐ Companies House or state registry entry matching name and DOB
- ☐ Social media profile cross-referenced with above
- ☐ Address history corroborated across at least two sources
- ☐ Photo confirmed via reverse image search if using an image
- ☐ Any aliases documented with sourced evidence (see Worksheet 12.2)
- ☐ No confusion with another individual of the same name confirmed

WORKSHEET 12.2

Alias Documentation Form

Confirmed Legal Name	Alias Used	Platform / Context	Source Documenting the Link	Date of Documentation

PART FOUR

Putting It Together

Building subject files, writing about what you find, working with others, and submitting to the institutions that have subpoena power.

CHAPTER 13

Building a Subject File

How to organize everything so it is usable, shareable, and defensible.

The investigation that is organized is the investigation that produces results. The research that lives in scattered screenshots, bookmarks, and memory produces nothing publishable. Before you start any investigation, set up the file structure. Before you add anything to it, use the three-category system. The time you spend on organization is not wasted — it is what lets you find the thing you need in six months when a new development makes it relevant.

The three categories — use them constantly

> **THE ONLY THREE CATEGORIES**
>
> *CONFIRMED — Verified from a named, citable public source. Publishable.*
> *ALLEGED / CLAIMED — Stated in a court filing, victim statement, or by a named individual. Publishable only when clearly labeled as such, with the source named.*
> *UNVERIFIED — You found it but cannot source it from a named public record. Not publishable. Keep researching or cut it.*

Your subject file folder structure

- **[Subject Name] / Documents** — PDFs of court filings, corporate records, 990s, government database exports
- **[Subject Name] / Screenshots** — Named per the convention in Chapter 3
- **[Subject Name] / Archives** — A text file with archive URLs, one per line, with a brief description of each
- **[Subject Name] / Notes** — A running document in your own words: what you know, what you suspect, what you still need to find, what questions are open
- **[Subject Name] / Published** — Final copies of anything you published, plus the date

The timeline

Build a dated timeline for every subject you investigate seriously. Every documented fact with a date goes in it. A timeline makes patterns visible — sudden corporate dissolutions, post spikes around key

events, patterns of contact that cluster around specific developments. The timeline is also your best defense against being told your analysis is backwards — the dates speak for themselves.

WORKSHEET 13.1

Subject File Master Template

Subject's confirmed legal name:

Known aliases (with sources):

Date of birth (if public record):

Nationality / residence:

Known addresses (from public records — source each):

Corporate entities associated (Companies House / state registry):

Court records (case numbers, jurisdictions, outcomes):

Government database findings (BOP, FEC, FAA, professional licenses):

Social media profiles (platform, username, follower count, date checked):

Documented connections to other subjects (with sources):

Epstein file appearances (EFTA document numbers, context):

Key confirmed findings summary:

Open questions / unverified leads:

WORKSHEET 13.2

Investigation Timeline Builder

Date	Event	Source (citable)	Category	Notes

CHAPTER 14

Writing About What You Find

The standard that separates a blog post from journalism that holds up.

The difference between what I write and what a lot of people in this space write is not that I have access to information they do not have. It is that I will not publish a claim I cannot source. That standard is inconvenient and often means you leave things out that you believe are true but cannot prove. It means you sometimes wait for a finding to be confirmed rather than publishing a lead but it also means that when the people you are writing about try to discredit you, they consistently fail — because the record shows that what you published was documented and what you called unverified you actually called unverified.

How to write about an allegation without becoming liable for it

The word "alleged" is not a magic shield, but used correctly it is a genuine legal protection. An allegation that comes from a named court filing or a named individual is publishable as an allegation. The formula is: "A victim statement in DOJ document EFTA01652016 alleges that [X]." That is accurate. That is citable. The key is that the allegation comes from the document, and you are reporting that the document contains it.

What you cannot do: present an unverified claim as fact, remove "alleged" from something you initially labeled as alleged, or take an allegation from one document and present it as corroborated by a second document that says something different.

Attribution — what "according to" means

"According to court filings" means you read the court filing and it says what you say it says. It does not mean someone told you about the court filing. You read the primary source and cite the primary source. You do not cite secondary reporting about the primary source unless the primary source is genuinely inaccessible — and even then, you note that you are citing secondary reporting and why.

When to contact a subject before publishing

The answer is: when your piece makes a significant specific claim about that person. You are not required to do this legally, in most jurisdictions, for reporting on public figures using public records. But it is good practice for three reasons: it sometimes produces a response that is itself newsworthy, it creates a documented record that you offered the person an opportunity to respond, and it

occasionally surfaces information that causes you to revise your understanding before publication rather than after.

Send the contact by email if you have it, by DM on a public platform if you do not. State clearly who you are, what you are publishing, and what specific claim you are seeking comment on. Set a reasonable deadline. Document the attempt and the outcome — response, no response, or cease-and-desist.

WORKSHEET 14.1

Pre-Publication Checklist

Run through this before every publication. Every box must be checked.

- ☐ Every claim in this piece has a named, citable source
- ☐ All allegations from court filings are labeled as allegations with the filing cited
- ☐ All unverified material has been removed or clearly labeled as unverified
- ☐ No home addresses of private individuals are published
- ☐ No information about minors is published
- ☐ Subject was contacted for comment (or a documented attempt was made)
- ☐ All key documents are archived at archive.today or Wayback Machine
- ☐ File naming convention applied to all supporting materials
- ☐ A co-investigator or trusted reader has reviewed the piece
- ☐ The piece has been read in full one final time with fresh eyes

WORKSHEET 14.2

Legal Threat Documentation Form

Date of threat:

Method (email / DM / letter):

From whom:

Full text of threat (or description if verbal):

What they are demanding:

My response (or planned response):

Attorney consulted:

RCFP contacted:

Outcome:

Did I continue publishing? What I published after the threat and when:

CHAPTER 15

Working With Others

Investigations like The Machine were not done alone.

The Machine series involved many people who sent information they had found or experienced. That collaboration produced things I may not have found working alone. It also required trust, clear agreements about what gets shared and what does not, and consistent communication about where I am in the investigation. This chapter covers how to do that well.

Vetting a potential co-investigator

Before you share anything sensitive with someone you plan to work with, ask: What is their track record? Have they published before — and was it accurate and sourced? Do they have a documented history of protecting sources? Have they been targeted by the people you are investigating, and if so, how did they handle it? Are their motives aligned with yours? "Aligned with yours" means they care about the accuracy and the accountability, not about being the person who breaks the story.

Information sharing protocols

- **Decide** before you begin what each person will and will not have access to. Who has source contact information? Who has the unverified leads file? Who can speak publicly about the investigation?
- **Communicate** securely. Signal for messages and ProtonMail for documents. Not SMS or regular email for sensitive material.
- **Establish** who makes the final publication decision. Disagreements about what to publish and when are inevitable. **Decide in advance how you resolve them.**

Source protection

If someone brings you information and asks to remain anonymous, the protection of that person is your professional obligation. It does not expire because the story gets hard or because someone is threatening you with legal action. The secure communication tools listed in Chapter 2 exist specifically for this. Use them from the first contact with any source who might have safety concerns.

WORKSHEET 15.1

Co-Investigator Working Agreement

Write this down and have both parties keep a copy before beginning any significant collaboration.

Investigator 1 name and contact:

Investigator 2 name and contact:

Scope of investigation (what we are working on together):

What each investigator will have access to:

How publication decisions will be made:

How attribution will be handled:

What happens if the collaboration ends:

Source protection agreement (both parties' commitment):

CHAPTER 16

How to Submit to Congress, the FBI, and the DOJ

Documented evidence deserves to go to the people with subpoena power.

One of the most common questions I get from people who have been following The Machine series is: what do I do with this? The answer is: you submit it. Not because you expect a call back or because you trust the institutions to act on their own. But because every documented, sourced submission that arrives at a congressional office creates a paper trail, and paper trails are what congressional investigations use when they decide what is worth pursuing with subpoena power.

The Machine investigation has produced a formal evidentiary submission delivered to congressional offices. That submission cites documented findings. It is not a complaint — it is a record — and you can contribute to that record.

Congressional submissions

Every member of Congress has a contact page at house.gov and senate.gov. The most relevant committees for this investigation are the House Judiciary Committee, the House Oversight Committee, and the Senate Judiciary Committee. Staff members on these committees read constituent submissions. A submission that is organized, sourced, and specific — naming the EFTA document numbers, case docket numbers, and platform archives that support each claim — is more likely to be read carefully than a general complaint.

The congressional contact tool at grifter-nation.com provides direct contact information and a template for submissions. Use it.

FBI tip portal

The FBI online tip portal is at tips.fbi.gov. Submissions are logged but are not always acted on and they are not always acknowledged. Submit anyway. A pattern of submissions about the same subjects from multiple people over time creates a documented record of public concern that is harder to ignore than a single submission.

What to include in any government submission

- **A** clear description of what you found and what you believe it shows
- **The** specific named sources: EFTA document numbers, court docket numbers, Companies House numbers
- **Archive** URLs for any social media content
- **A** statement of how you obtained the information (public records, not hacking)
- **Your** contact information if you are willing to be contacted

WORKSHEET 16.1

Government Submission Tracker

Agency / Office	Submission Date	Method	Confirmation #	Subject of Submission	Key Documents Cited	Response Received

PART FIVE

Reference Materials

The complete tool directory, glossary, and quick-reference cards. Keep this section open while you work.

CHAPTER 17

The Complete Tool Directory

Every tool in this workbook. Updated at followthefiles.com/tools.

The tools listed here were current and accurate at the time this workbook was published. URLs change, platforms update their interfaces, and new tools become available and old ones are retired. The living version of this directory — updated whenever something changes — is at followthefiles.com/tools. Before relying on any tool listed here for active investigation, verify the current URL and status at the site.

Court Records

TOOL
PACER

pacer.gov

Federal court electronic records system. Every federal civil and criminal case. Complaints, motions, orders, judgments.

Cost: Free account / $0.10 per page (waived under $30/quarter) · Best for: Federal case research

TOOL
CourtListener

courtlistener.com

Free mirror of significant PACER content plus full-text opinions. Operated by the Free Law Project.

Cost: Free · Best for: Fast federal case search without PACER cost

TOOL
CourtReference

courtreference.com

State-by-state directory of court search portals. Maintained regularly.

Cost: Free · Best for: Finding the right state court search tool

Corporate Records

TOOL
UK Companies House

gov.uk/government/organisations/companies-house

UK government registry of all limited companies. Officers, shareholders, filing history, accounts.

Cost: Free · Best for: UK corporate network research

TOOL

OpenCorporates

opencorporates.com

Aggregates corporate records from 140+ jurisdictions worldwide. Single search across countries.

Cost: Free (basic) / Paid (bulk) · Best for: Multi-jurisdiction corporate search

TOOL

Wyoming SOS

wyobiz.wyo.gov

Wyoming Secretary of State business search. Key for shell company research.

Cost: Free · Best for: Wyoming LLC and shell company research

TOOL

Delaware Corps

icis.corp.delaware.gov

Delaware Division of Corporations entity search.

Cost: Free · Best for: Delaware entity status and registered agent

Nonprofit Records

TOOL

ProPublica Nonprofit Explorer

projects.propublica.org/nonprofits

990 tax filings for all US nonprofits. Revenue, compensation, board members, activities. Searchable by name or EIN.

Cost: Free · Best for: 990 analysis and nonprofit revenue research

TOOL

IRS Tax Exempt Search

apps.irs.gov/app/eos

IRS official tax-exempt status lookup. Confirms current status.

Cost: Free · Best for: Verifying 501(c)(3) status

TOOL

Candid (GuideStar)

candid.org

Foundation and nonprofit database. Good for grant recipient research.

Cost: Free (basic) / Paid · Best for: Foundation grant tracking

Government Databases

TOOL

BOP Inmate Locator

bop.gov/inmateloc

Federal Bureau of Prisons public inmate locator. Searches by name or Register Number.

Cost: Free · Best for: Confirming federal inmate status and BOP Register numbers

TOOL

FEC.gov

fec.gov/data

Federal Election Commission records. Political contributions, PAC filings, donor records.

Cost: Free · Best for: Political money connections

TOOL

FAA Registry

registry.faa.gov

Aircraft ownership by tail number or owner name. Foundation of flight log analysis.

Cost: Free · Best for: Aircraft ownership confirmation

TOOL

ProPublica Trump Town

projects.propublica.org/trump-town

Database of Trump administration personnel with salaries and dates.

Cost: Free · Best for: Confirming White House staffing records

TOOL

Muckrock

muckrock.com

FOIA request filing and tracking platform. Published database of completed requests.

Cost: Free (basic) / Paid (more requests) · Best for: FOIA requests and browsing others' completed requests

Epstein Files

TOOL

DOJ Epstein Library

justice.gov/epstein

Official DOJ repository for all Epstein file releases.

Cost: Free · Best for: Primary source for Epstein documents

TOOL

Epstein Data

epstein-data.com

Community-built full-text search across released Epstein documents.

Cost: Free · Best for: Keyword searching across the Epstein files

TOOL

EpsteinGraph

epsteingraph.com

Relationship mapping tool built from the Epstein files.

Cost: Free · Best for: Visualizing connections in the files

Archiving

TOOL

Wayback Machine

web.archive.org

Internet Archive's web archiving service. Submit URLs to archive. Browse historical snapshots by date.

Cost: Free · Best for: Archiving URLs and recovering deleted content

TOOL

Archive.today

archive.ph

Fast URL archiving with good social media capture. Generates a permanent archive URL.

Cost: Free · Best for: Social media post archiving

Identity and Background

TOOL

BeenVerified

beenverified.com

Consumer background check aggregator. Addresses, phone numbers, associates, aliases. Use for leads, not confirmation.

Cost: Paid subscription · Best for: Generating leads on addresses and associates

TOOL

TinEye

tineye.com

Reverse image search. Upload a photo to find where it appears online.

Cost: Free (limited) / Paid · Best for: Verifying profile photo identity

TOOL

Yandex Images

yandex.com/images

Often surfaces results that Google Image Search misses. Strong facial recognition in reverse search.

Cost: Free · Best for: Reverse image search for faces

Secure Communication

TOOL
Signal

signal.org

End-to-end encrypted messaging and calls. The standard for secure source communication.

Cost: Free · Best for: Secure messaging with sources and co-investigators

TOOL
ProtonMail

proton.me

Encrypted email. Better than regular email for sensitive document exchange.

Cost: Free (basic) / Paid · Best for: Secure email communication

TOOL
ProtonVPN

protonvpn.com

VPN with a free tier. Swiss-based, no-logs policy.

Cost: Free (limited) / Paid · Best for: Baseline VPN privacy for research

Legal Resources

TOOL
RCFP Legal Defense

rcfp.org

Reporters Committee for Freedom of the Press. Legal hotline for journalists: 1-800-336-4243.

Cost: Free · Best for: First call when you receive a legal threat

TOOL
EFF Legal Guide

eff.org/issues/blogger

Electronic Frontier Foundation guide for bloggers and independent journalists on legal rights.

Cost: Free · Best for: Understanding your legal rights before you publish

CHAPTER 18

Glossary of Terms

Every term used in this workbook, defined clearly.

Legal Terms

Allegation A claim made in a legal filing or by a named individual that has not been proven in court. Must be labeled as such when reported.

Anti-SLAPP Strategic Lawsuit Against Public Participation. Laws in many states that allow defendants to quickly dismiss frivolous lawsuits filed to silence public comment. "Totally devoid of merit" is language from an anti-SLAPP ruling.

Civil Dismissal With Prejudice A case dismissed in a way that prevents it from being refiled. Does not indicate innocence.

Complaint The initial filing in a civil lawsuit that describes the plaintiff's allegations. It is the plaintiff's story under oath — not a finding of fact.

Contempt of Congress Refusal to comply with a congressional subpoena. Can result in criminal charges.

Docket The running index of all filings in a court case, with dates.

Motion to Dismiss A request by a defendant to have a case thrown out before trial. Denial means the court found the claims sufficiently valid to proceed.

PACER Public Access to Court Electronic Records. The federal government's public court document portal.

Preponderance of the Evidence The civil standard of proof. More likely than not — a lower bar than "beyond a reasonable doubt."

Subpoena A court order requiring someone to testify or produce documents. Only institutions with legal authority can issue subpoenas.

Corporate Terms

Correspondent Address In UK Companies House filings, the address where legal correspondence is sent. Can differ from the registered office.

Dissolved A UK or US company that has been formally removed from the register. Its filing history remains public.

EIN Employer Identification Number. The US federal tax identifier for businesses and nonprofits. Required on 990 filings.

Person with Significant Control (PSC) UK Companies House term for major shareholders (holding 25%+ of shares or voting rights).

Registered Agent A person or company designated to receive legal documents on behalf of a business entity. Many shell companies use professional registered agents at generic addresses.

SIC Code Standard Industrial Classification. A code describing a company's business activity. "Other business support service activities n.e.c." is a catch-all code that tells you little.

Investigative Terms

Chain of Evidence A documented, unbroken record connecting a finding to its source. Every link in the chain must be citable.

Dox / Doxxing Publicly publishing private personal information — home address, phone number, family details — about an individual, typically to enable harassment. This workbook does not encourage it and instructs against it.

EFTA Document Number The designation system for documents released under the Epstein Files Transparency Act. EFTA followed by a number (e.g., EFTA01652016).

FOIA Freedom of Information Act. The US federal law giving citizens the right to request government records.

OSINT Open-Source Intelligence. The practice of gathering information from publicly available sources.

Primary Source The original document, filing, or record — not a secondary report about it. Always cite primary sources when possible.

Sockpuppet A fake social media account used to amplify content or harass individuals while concealing the real identity behind it.

The Machine — Specific Terms

The Machine The documented network operating to rehabilitate Ghislaine Maxwell's public image and attack the credibility of Epstein survivors. Documented in The Machine series at thefalloutwithtbs.substack.com.

EFTA01652016 A specific 24-page DOJ federal witness harassment complaint released under the Epstein Files Transparency Act, naming Ghislaine Maxwell, George B. Tonks, Garrett Ziegler, David Boies, and 22 others.

BOP Register Number The Federal Bureau of Prisons inmate registration number. Verifiable at bop.gov/inmateloc.

CHAPTER 19

Quick Reference Cards

Print these. Keep them where you work.

CARD 1: PRE-PUBLICATION — EVERY CLAIM SOURCED?

- Every claim has a named, citable source
- Allegations from filings labeled as allegations with filing cited
- All unverified material removed or clearly labeled
- No home addresses of private individuals published
- No information about minors published
- Subject contacted for comment (or attempt documented)
- All key documents archived at archive.today or Wayback

CARD 2: WHAT TO CAPTURE IN EVERY SCREENSHOT

- Full URL visible in browser address bar
- Account username clearly visible
- Verification status visible
- Follower count if shown on page
- Date and time of post
- Full text — do not crop
- Engagement counts at time of screenshot
- Then archive at archive.today

CARD 3: TOP DATABASES WITH URLS

- PACER (federal courts): pacer.gov
- CourtListener (free federal): courtlistener.com
- UK Companies House: gov.uk/government/organisations/companies-house
- ProPublica Nonprofit Explorer: projects.propublica.org/nonprofits
- BOP Inmate Locator: bop.gov/inmateloc
- FAA Aircraft Registry: registry.faa.gov
- FEC Political Money: fec.gov/data
- DOJ Epstein Files: justice.gov/epstein
- Epstein-Data Search: epstein-data.com
- All links maintained at: followthefiles.com/tools

CARD 4: LEGAL THREAT RESPONSE STEPS

- Step 1: DO NOT DELETE ANYTHING
- Step 2: Screenshot and save the threat with date and time
- Step 3: Do not respond without consulting an attorney
- Step 4: Call RCFP Legal Defense Hotline: 1-800-336-4243
- Step 5: Document everything — the threat, your response, what you published after
- Step 6: Continue publishing if the work is sound

CARD 5: CONGRESSIONAL CONTACT QUICK GUIDE

- House Judiciary Committee: judiciary.house.gov
- House Oversight Committee: oversight.house.gov
- Senate Judiciary Committee: judiciary.senate.gov
- Your representatives: house.gov and senate.gov
- Congressional contact tool with templates: grifter-nation.com
- FBI tip portal: tips.fbi.gov
- Include: EFTA document numbers, case docket numbers, archive URLs

PART SIX

Why This Lane Is So Important

The files are out, the conversation is happening, and most of it is looking at the wrong thing.

CHAPTER 20

The Files vs. The Machine

What the public conversation got right, what it missed, and why that gap is the whole problem.

Let me tell you what I have watched happen since the Epstein files were released.

People who have been paying attention for years — people who followed the Maxwell trial, who read the victim statements when they were unsealed, who understood what the network actually was — finally got something they could point to. Three million documents, emails, photos, flight logs, contact books, and names. Names that everybody knows. The conversation that followed was enormous and it was legitimate. Accountability for the people who were part of Epstein's world is the whole point.

But somewhere in that conversation, something happened. The attention moved entirely to what the files contained and away from what is still happening. The people who put Maxwell in prison are being harassed right now — not in the past — right now, today, as you read this. The people running that harassment operation are not in the flight logs, were not at the parties, nor are they celebrities. They are mainly on X and Telegram and Substack, with large audiences, with verified checkmarks, with documentary deals and podcast appearances, and they are describing Maxwell's conviction as an American disgrace and her victims as pathological liars. They are named in federal documents about this, and those documents are in the same file dump everyone is reading.

Most people who are paying attention to the files have not opened those documents.

That is the gap. That is why this workbook and The Machine series exists. Do not be mistaken, though, I am not saying that the names-in-the-files conversation is wrong — it isn't — but because it is incomplete, and the part that is missing is the part that is still running.

What the machine does

I have, thus far, spent twenty-two parts of this series documenting it in detail, so I am going to be precise here rather than general. The machine does three specific things.

First, it rehabilitates Maxwell's narrative. Maxwell is in federal prison, convicted by a jury after only six hours of deliverabtion. She cannot speak directly to the public without her communications being monitored and potentially subpoenaed. So the narrative rehabilitation happens through proxies — a woman who confirmed she speaks with Maxwell by phone visiting from Florida, who broadcasts Maxwell's framing to 568,000 Instagram followers, who describes Andrew Mountbatten-Windsor's

presence in the Epstein files as "an honour, not a shame," who posted KARMA over a dying Virginia Giuffre's photograph. That is a documented, named, sourced operation running right now.

Second, it attacks the credibility of survivors. The specific target is the people whose testimony put Maxwell away. Maria Farmer, Virginia Giuffre, and the women whose accounts are in the court record. The machine's job is to make those accounts look fabricated, coordinated, extortionate, or politically motivated. When that framing reaches a million-follower audience without scrutiny, it does damage that cannot be easily undone.

Third, it exploits the information environment. The same spaces where people go to find out what is really happening in the Epstein case — because they correctly do not trust institutional media to cover it fully — are the spaces where the machine operates. People looking for truth in a space that is not properly filtered encounter the machine and cannot always tell the difference between independent investigation and coordinated narrative management. That is not an accident at all, it is the design.

Why open-source investigators are specifically positioned to see this

The machine operates on the assumption that nobody is looking carefully enough. It relies on the fact that most people who encounter a Substack with 77,000 subscribers and a blue checkmark and a polished logo will not pull up the federal conviction record, the BOP register number, the court documents showing $1.57 million in unpaid restitution, and the text messages showing coordination with a White House aide who ended up in a DOJ witness harassment complaint. Those things are all in public databases and are all findable by anyone who knows where to look.

The institutional media has largely failed this story — and I am not saying that journalists are corrupt but that the the story requires sustained, detailed, technical research that does not fit the news cycle and that does not produce the kind of headline that gets clicks without context. The people who are positioned to do that work are the independent investigators who know how to navigate PACER and Companies House and the Epstein file repositories and who have the time and the motivation to follow something for months rather than hours.

That is you. If you have read this far, **that is you.**

What it will actually take

I want to be honest about this because I think people are waiting for a moment that resolves things — a final document release, an arrest, a congressional hearing that changes everything. That moment may come, but the pattern of this investigation suggests that what changes things is not a single event but accumulated pressure from documented findings. The documented record of what Tonks has

done was built piece by piece over many months and with twenty years of knowing him. The EFTA document naming him and Ziegler alongside Maxwell was not created by a reporter or a documentary filmmaker. The only reason that document exists is because someone submitted to the DOJ and the submission went into the record and the record eventually got released under a transparency act that passed because Congress felt public pressure to pass it.

The submission you make from Chapter 16 of this workbook is one piece, the investigation you document is one piece, and the piece you publish using the standards in Chapter 14 is one piece. Individually none of these things end the machine but, together, sustained over time, they create the accumulated documented record that makes it harder and harder for the machine to operate without consequence. That is the work and the work is definitely not fast, but it is the work that actually matters.

CHAPTER 21

The Companion Website

What followthefiles.com is, what it has, and how to use it alongside this book.

---

followthefiles.com is the living version of this workbook. Everything in here that has a web equivalent lives there — updated when URLs change, expanded when new tools become available, and connected to the active investigation documented in The Machine series.

What you will find there

- **The Living Tool Directory** — Every tool in Chapter 17, maintained with current URLs and any changes to pricing or interface. If a link in this workbook is broken, the current version is there.
- **Worksheet Downloads** — Every fillable worksheet in this book available as a standalone PDF. Print extras and share them.
- **The Updates Page** — A running log of anything in the workbook that has changed since publication with dated entries. Check it periodically.
- **The Machine Context** — The argument for why this lane of investigation matters, with links to the full series at thefalloutwithtbs.substack.com.
- **Congressional Contact Tool** — Direct contact to the relevant committees and offices with submission templates. The same tool at grifter-nation.com.
- **SA Support Website** — the grifter-nation.help . Share it.

The workbook is the foundation. The site is what keeps it from becoming outdated. Use both.

CHAPTER 22

Pay What You Can

The suggested price for this workbook is $10.

That amount directly supports the ongoing investigation documented in The Machine series — the records requests, the database subscriptions, the time it takes to pull and cross-reference the findings that end up in twenty-two parts of documented reporting and counting. If you can pay it, please do.

If you cannot pay anything at all — if money is genuinely a barrier — take it and use it well. That is not a burden or an afterthought because the work that you do with these tools is worth more than the price of the workbook. The information matters more than the transaction. Use it responsibly and use it to contribute something to the record.

The only thing asked of everyone who uses this — regardless of what they paid — is this: do the work carefully. Verify before you publish, label what you know and label what you do not know, always protect your sources, submit what you find to the people with the power to act on it, and keep going.

ABOUT THE AUTHOR

Troy Barile

Troy Barile is an investigative journalist and the author of The Machine, a twenty two-part series, and growing, documenting the network operating to rehabilitate Ghislaine Maxwell's public image and attack the credibility of Epstein survivors. The series is published at thefalloutwithtbs.substack.com and has reached readers across thirty-plus countries. His work has generated formal evidentiary submissions to congressional offices and has been cited by readers, researchers, and attorneys working on matters connected to the Epstein case.

He is the founder of grifter-nation.com, a resource for survivors, advocates, and investigators, and grifter-nation.help, a survivor support and resource directory. He is a regular contributor to WhoWhatWhy.org with a weekly series on Jeffrey Epstein.

He is not a trained journalist, learned to do this by doing it, and built this workbook because the tools and methods that produced The Machine series should not stay with one person.