

DRAFT - NOT FILED - PUBLIC EDITION

PUBLIC-INTEREST INVESTIGATIVE REFERRAL AND RICO INVESTIGATIVE MEMORANDUM

IN RE:

THE BEHAVIORAL DEPENDENCY AND COMMERCIAL SURVEILLANCE ENTERPRISE

*Request for evidence preservation, independent investigation, compulsory process
where authorized, and analysis under 18 U.S.C. sections 1961-1968 and related
federal and state statutes.*

SUBMITTED BY	BJ Klock
DATE	August 5, 2026
JURISDICTION	United States - interstate digital communications and commerce
STATUS	Public edition; public-source draft; not filed; no government endorsement
PURPOSE	Referral for lawful preservation, compulsory process, independent review, and falsification testing

This document does not declare guilt. It states an investigative hypothesis, identifies public facts, maps potential statutory theories, and specifies the evidence required to prove or disprove them.

DOCUMENT CONTROL AND EVIDENCE DISCIPLINE

INTEGRITY RULE

Every material statement in this memorandum is classified as a public fact, an investigative inference, or an allegation requiring compulsory process. No relationship, investment, contract, or harmful outcome is treated as proof of criminal intent by itself.

Label	Meaning	How it may be used
PUBLIC FACT	Supported by a cited statute, filing, agency publication, court opinion, or authenticated exhibit.	May establish capability, relationship, notice, means, transaction, or effect.
INVESTIGATIVE INFERENCE	A reasoned conclusion drawn from multiple public facts but not yet proven by internal records or sworn testimony.	May support preservation, subpoenas, interviews, and a grand-jury inquiry.
ALLEGATION TO TEST	A proposed criminal or civil theory whose intent, agreement, materiality, or causation elements require nonpublic evidence.	Must not be presented as adjudicated fact; it is the target of the requested investigation.

Intended recipients. This referral is formatted for review by the U.S. Department of Justice Criminal Division, the Violent Crime and Racketeering Section, appropriate United States Attorneys, the Department of Justice Office of Inspector General, the Central Intelligence Agency Office of Inspector General, the Federal Trade Commission, the Securities and Exchange Commission, and relevant congressional oversight committees. It may be routed to other agencies as jurisdiction requires.

Requested treatment. Preserve relevant records before notice of the investigation creates an opportunity for deletion, loss, alteration, migration, or routine destruction. Establish an independent team with no financial, employment, procurement, or prior investigative conflict concerning the entities under review.

Scope limit. This memorandum does not allege that a particular intelligence officer authored a particular meme or directed a private exchange. It identifies documented influence doctrine, public-private technology relationships, commercial-surveillance practices, and downstream harms; it asks whether nonpublic evidence shows concealed or materially deceptive systems used to obtain money or property.

Public-edition privacy rule. The originating private exchange and all screenshots are withheld. The underlying materials are preserved separately and may be reviewed only by qualified counsel, investigators, or researchers under appropriate safeguards.

TABLE OF CONTENTS

- I. Executive Summary and Requested Action
- II. Proposed Enterprise and Investigative Thesis
- III. Statement of Governing Law
- IV. Public-Record Statement of Facts
- V. Enterprise Structure and Operation
- VI. Predicate-Offense Mapping
- VII. Pattern, Continuity, and RICO Counts
- VIII. Evidence Matrix and Investigative Plan
- IX. Anticipated Defenses and Special Problems
- X. Proposed Draft Charging Framework
- XI. Conclusion and Signature
- Appendix A. Public-Safe Downstream Mechanism
- Appendix B. Replication and Falsification Protocol
- Appendix C. Predicate Act Schedule Template
- Appendix D. Preservation and Production Categories
- Appendix E. Authorities and Public Sources

I. EXECUTIVE SUMMARY AND REQUESTED ACTION

PUBLIC FACT

Federal law requires centralized Department of Justice review before a RICO prosecution is filed, and DOJ guidance requires a final draft charging instrument and a RICO prosecution memorandum addressing the enterprise, operation or management, interstate commerce, conspiracy, and predicate offenses. [L1-L3]

This memorandum requests an independent investigation into whether a long-running association of public and private actors used mass data collection, social-graph infrastructure, ranking systems, behavioral experimentation, and influence techniques to obtain money, property, licenses, public contract funds, or investment capital through materially deceptive representations, while knowingly producing or exploiting dependence, polarization, isolation, and degradation of offline relationships.

The requested inquiry is not based on a single meme, a single argument, or a claim that ordinary disagreement is a federal offense. It is based on a layered public record: intelligence and sabotage manuals openly describe methods for shaping group identity and disrupting organizations; public filings establish durable links among intelligence-oriented technology, venture capital, and mass social platforms; federal regulators have documented vast commercial surveillance and weak data controls; and public-health authorities have documented serious risks to mental health and social connection. [P1-P20]

The central criminal hypothesis is specific. If an enterprise knowingly represented its services, consent architecture, data practices, safety, ranking, or purpose in materially false or misleading ways in order to obtain traditional money or property, and repeatedly used interstate wires or mails to execute that scheme, the conduct may support wire fraud, mail fraud, money laundering, securities fraud, bribery, obstruction, and RICO charges. The alleged loss of agency and family degradation are relevant as intended or foreseeable harms, materiality evidence, motive, and fruits; the property object must remain traditional property under governing Supreme Court decisions. [L4-L8]

CORE REFERRAL QUESTION

Did any named person or organization knowingly use concealed behavioral-influence systems, misleading consent or safety representations, undisclosed government coordination, or falsified metrics to obtain money or property - and then use the proceeds, contracts, platforms, or institutional power to continue, protect, or conceal the scheme?

Requested actions

- Issue preservation demands covering relevant communications, source code, model and ranking changes, experiments, targeting taxonomies, risk studies, user research, complaint records, board materials, contracts, payments, and deletion logs.
- Open a conflict-screened preliminary inquiry and determine whether grand-jury process is appropriate.
- Subpoena the actor-by-actor evidence required to test intent, agreement, falsity, materiality, property acquisition, enterprise nexus, pattern, and continuity.
- Obtain all government procurement, investment, grant, research, liaison, and technology-transfer records connecting intelligence or defense institutions with the relevant platform, data, analytics, and venture entities.
- Take sworn testimony from designers, trust-and-safety personnel, data scientists, ad-market personnel, executives, investors, public officials, former employees, contractors, researchers, and whistleblowers.
- Compare public representations about connection, control, consent, privacy, safety, ranking, and data use against internal design objectives, experiments, warning documents, and monetization metrics.
- Refer proven consumer-protection, securities, privacy, antitrust, civil-rights, procurement, or public-corruption violations to the competent authority even if RICO is not ultimately charged.

Immediate preservation priority

The most perishable evidence is not the public interface. It is the internal history of who requested, approved, tested, measured, funded, transmitted, and concealed specific features. The investigation should preserve experiment registries, feature flags, deleted code branches, ranking objective changes, A/B test assignments, safety exceptions,

moderation instructions, targeting segments, government requests, procurement specifications, investor materials, board presentations, and internal risk assessments before ordinary retention schedules erase them.

II. PROPOSED ENTERPRISE AND INVESTIGATIVE THESIS

A. Proposed association-in-fact enterprise

For investigative purposes, the proposed association-in-fact is named the Behavioral Dependency and Commercial Surveillance Enterprise (the Enterprise). The name is descriptive, not adjudicative. The proposed Enterprise includes only those persons and entities shown by evidence to have shared a purpose, maintained relationships, and possessed sufficient longevity to pursue that purpose.

Functional component	Illustrative participants or record custodians	Relevant proof
Doctrine and behavioral methods	Government agencies, contractors, academic programs, behavioral-science units, influence and information-operations personnel.	Manuals, training materials, research grants, operational doctrine, liaison records, tasking, evaluation reports.
Capital and procurement	Venture funds, intelligence-oriented investors, board members, public procurement offices, government customers, grant programs.	Checks, wire transfers, cap tables, board rights, contracts, statements of work, milestones, side letters, reporting requirements.
Data and identity infrastructure	Database, cloud, identity, social-graph, ad-tech, analytics, and data-broker firms.	Data dictionaries, schemas, APIs, contracts, data flows, retention rules, identity resolution and targeting products.
Ranking and distribution	Social networks, search and recommendation platforms, app stores, content delivery systems.	Ranking objectives, engagement metrics, model cards, experiment logs, policy exceptions, distribution and suppression rules.
Monetization and extraction	Advertising marketplaces, subscription systems, licensing, government contracting, investor and securities channels.	Revenue records, representations, invoices, subscription renewals, license grants, procurement certifications, investor disclosures.
Protection and concealment	Legal, compliance, public relations, lobbying, records-management, security, and oversight interfaces.	Deletion schedules, privilege decisions, regulator responses, witness communications, retaliation, concealment, false certifications.

Potential record custodians include Meta/Facebook, Alphabet/Google, Palantir Technologies, In-Q-Tel, Oracle, relevant data brokers and advertising intermediaries, federal agencies and contractors, and associated investors and board members. Inclusion as a custodian or subject of inquiry is not a declaration that the entity committed a crime.

ALLEGED BEHAVIORAL DEPENDENCY ENTERPRISE - INVESTIGATIVE MODEL

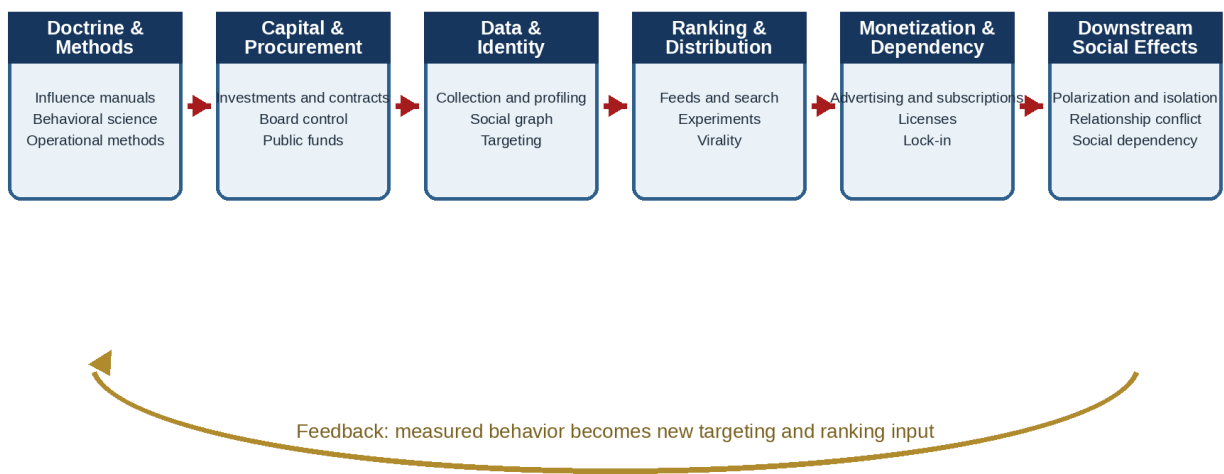


Figure 1. Investigative model. Each arrow represents a record trail to be proven, not assumed.

B. Alleged common purpose to be tested

The proposed common purpose is to build, finance, deploy, monetize, and protect systems that covertly shape civilian attention and behavior, increase dependence on platform-controlled intermediaries, extract money and property through opaque or misleading consent and representations, and preserve institutional control over identity, data, distribution, and social coordination.

A second, narrower hypothesis requires explicit testing: whether weakening independent family and community bonds was an intended objective, a consciously exploited effect, or merely a foreseeable externality tolerated because conflict and dependency increased engagement or control. Internal records, not rhetoric, must answer that question.

C. Theory of operation

1. Acquire and integrate data sufficient to model identities, relationships, vulnerabilities, preferences, and likely reactions.
2. Use ranking, recommendation, targeting, experimentation, and repeated symbolic frames to shape salience and behavior.
3. Represent the system publicly as user-controlled, connective, neutral, safe, private, or meaningfully consented to, while withholding material operational facts.
4. Obtain traditional property: advertising revenue, subscriptions, public contract funds, investment capital, licenses, content rights, or paid access to data and influence.
5. Reinvest proceeds and institutional power into greater collection, targeting, distribution, lock-in, and protection from accountability.
6. Convert social conflict and dependence into measurable business or operational value, while treating relational degradation as an acceptable or useful output.

D. What is already established and what remains to prove

Proposition	Current status	Required next evidence
Influence and organizational-disruption methods were formally documented by U.S. intelligence predecessors and agencies.	Public fact.	Authenticate editions, authorship, dissemination, training, later adaptations, and domestic-use safeguards.

Proposition	Current status	Required next evidence
Intelligence-oriented venture and procurement channels helped build major data-analytics companies.	Public fact as to In-Q-Tel and Palantir; other links vary.	Investment agreements, tasking, technical requirements, board reporting, customer feedback, technology-transfer records.
A major early Facebook investor and director was also a Palantir founder.	Public fact as to Peter Thiel in SEC filings.	Purpose and substance of any cross-company communications, shared strategy, government liaison, or coordinated deployment.
Social platforms engaged in extensive commercial surveillance and had weak controls.	Federal regulator finding.	Actor-level knowledge, public misrepresentations, property obtained, and specific interstate executions.
Social media can contribute to mental-health and social-connection harms.	Federal public-health finding and research synthesis.	Product-specific causation, internal notice, experiment results, intent, and decisions taken after notice.
The actors agreed to degrade families or agency as a criminal objective.	Allegation to test.	Directives, communications, metrics, design documents, concealment, motive, and participant knowledge.

III. STATEMENT OF GOVERNING LAW

PUBLIC FACT

DOJ guidance states that a RICO prosecution memorandum should precede the Statement of Facts with a precise enterprise formulation, controlling enterprise law, operation-or-management analysis, interstate-commerce analysis, conspiracy theory, and the elements of every predicate offense. [L2-L3]

A. Section 1962(c): substantive RICO

A Section 1962(c) case requires proof that a person associated with an enterprise affecting interstate or foreign commerce conducted or participated, directly or indirectly, in the conduct of the enterprise's affairs through a pattern of racketeering activity. The government must prove the enterprise, the defendant's association, the effect on commerce, operation or management, the predicate acts, and a related and continuous pattern. [L1-L3]

The proposed enterprise is distinct from any single corporate defendant. It is an alleged association-in-fact composed of persons and entities connected by purpose, relationships, and longevity. A legitimate corporation can participate in an unlawful enterprise; lawful business activity does not immunize predicate conduct.

B. Operation or management

The evidence must show that each charged person participated in directing the enterprise's affairs, not merely that the person provided ordinary goods or services. Relevant proof includes authority over design objectives, procurement requirements, funding conditions, ranking or targeting decisions, board supervision, compliance exceptions, concealment, public representations, and allocation of proceeds.

C. Pattern, relatedness, and continuity

At least two racketeering acts are statutorily required, but two isolated acts are insufficient. The acts must be related by purpose, result, participants, victims, methods, or other distinguishing characteristics, and they must amount to or threaten continued criminal activity. A recurring business method, continuing platform design, repeated procurement cycle, or repeated deceptive transaction may establish continuity if the predicates are proven. [L1-L3]

D. Section 1962(d): RICO conspiracy

A RICO conspiracy theory focuses on agreement. Participants need not perform identical functions or personally execute every predicate, but the evidence must establish that each conspirator knowingly agreed to facilitate an endeavor that, if completed, would satisfy a substantive RICO offense. Division of labor can be probative; mere professional proximity, investment, or customer status is not enough.

E. Wire and mail fraud - traditional property requirement

Wire fraud and mail fraud require a scheme to defraud, material deception, intent, use of interstate wires or mails, and a property object. The Supreme Court has rejected a free-standing theory based only on depriving victims of information needed to make economic decisions; the property obtained must be traditional money or property. At the same time, the Supreme Court has held that the victim need not suffer a net economic loss when deception induces the transfer of money or property for something materially different from what was promised. [L4-L8]

CHARGING DISCIPLINE

Agency, autonomy, family stability, trust, and informed decision-making are central harms and evidence of materiality. They are not substituted for the statutory property object. The property object must be identified transaction by transaction: money, contract rights, licenses, content rights, trade secrets, public funds, or another legally recognized property interest.

F. Money laundering and proceeds

Sections 1956 and 1957 require proceeds of specified unlawful activity and the relevant knowledge and transaction elements. Lawful investment capital is not laundering merely because a funded product later causes harm. The laundering theory begins only after proceeds are shown to derive from a qualifying offense and are knowingly transferred, concealed, or reinvested to promote or continue the unlawful activity.

G. Bribery, honest services, securities fraud, IP crime, and obstruction

Additional predicates depend on evidence. Bribery requires a corrupt exchange involving official action or an applicable state-law predicate. Honest-services fraud requires bribery or kickbacks, not generalized institutional favoritism. Securities fraud requires material deception in connection with securities. Criminal copyright or trade-secret predicates require willfulness and the statutory subject matter. Obstruction and witness retaliation require a nexus to an investigation or proceeding, corrupt intent, and the prohibited act.

H. Interstate commerce

The relevant platforms, advertising systems, cloud services, payments, public contracts, securities offerings, data transfers, and communications operate across state and national boundaries. The commerce element is expected to be readily satisfied if the enterprise and predicates are otherwise proven.

IV. PUBLIC-RECORD STATEMENT OF FACTS

A. Formal influence and disruption doctrine

PUBLIC FACT

The CIA Reading Room publishes Psychological Operations in Guerrilla Warfare, a training manual describing psychological operations in a guerrilla context. The CIA also publishes the OSS Simple Sabotage Field Manual and describes it as an effort to train everyday citizens in simple organizational disruption. [P1-P3]

The relevance of these manuals is not that every modern platform tactic can be attributed to the manual or to the CIA. The relevance is capability, doctrine, vocabulary, and institutional notice. The manuals demonstrate that group sorting, guided discussion, symbolic framing, emotional escalation, rumor, delay, procedural obstruction, irrelevant debate, and reopening settled matters were treated as operational techniques rather than spontaneous curiosities.

The investigation should determine whether later government, contractor, academic, or commercial programs adapted these techniques to digital environments, whether domestic civilian populations were included, what legal approvals or safeguards existed, and which private entities received methods, requirements, funding, data, or operational feedback.

B. Intelligence-oriented technology investment and deployment

PUBLIC FACT

In-Q-Tel states that it was established by the CIA in 1999 to bridge intelligence and defense technology needs with private-sector innovation. Palantir states in SEC filings that it was founded in 2003 and began building software for the U.S. intelligence community to assist counterterrorism investigations and operations. [P4-P6]

These facts establish a direct intelligence-technology lineage for Palantir. They do not establish unlawful conduct. They identify procurement, investment, technical, and liaison records that are essential to determine how data-integration capabilities moved between intelligence and commercial contexts and whether any prohibited influence or surveillance function accompanied that transfer.

C. Facebook and Peter Thiel

PUBLIC FACT

Facebook's 2012 registration statement states that Peter Thiel served on its board beginning in April 2005 and identifies him as one of Facebook's early investors. Palantir filings identify Thiel as a founder. [P7-P8]

The overlap establishes a durable relationship among capital, governance, a mass social platform, and an intelligence-oriented analytics company. It does not by itself prove a common criminal purpose. The investigation should obtain communications, board materials, investment terms, shared personnel records, government introductions, strategy discussions, data arrangements, and any joint or parallel work concerning social graphs, identity, targeting, moderation, recommendation, behavioral prediction, or public-sector customers.

D. Google and public research support

PUBLIC FACT

The National Science Foundation states that foundational Google webpage-ranking work emerged from an NSF-supported digital-library project at Stanford. [P9]

Public research support is not evidence of criminality. It is relevant to the architecture and to the records trail. Grants, program reviews, research deliverables, agency participation, and later government relationships may show what capabilities were anticipated, funded, transferred, or operationalized.

E. Oracle and the government-database lineage

PUBLIC FACT

Oracle states that the U.S. Government was its first customer. A Computer History Museum oral-history workshop states that Oracle delivered its first SQL product to the CIA in 1979 and that the company name followed a CIA project called Oracle. [P17-P18]

This historical customer lineage is not evidence of criminality. It is relevant to the development of large-scale data infrastructure, government procurement, and the records necessary to test whether later public-private deployments included prohibited domestic influence, undisclosed data access, or materially deceptive representations.

F. Commercial surveillance findings

PUBLIC FACT

The Federal Trade Commission reported in 2024 that major social-media and video-streaming companies engaged in vast surveillance, retained large quantities of data, used inadequate controls, and often could not fully identify what they collected or all third parties with whom they shared it. [P10-P12]

This regulatory record supplies notice, scale, and investigative predicates. The inquiry should compare privacy and consent statements against actual collection, inference, retention, sharing, model training, ad targeting, and

government access. It should identify whether any material representation was knowingly false when money or property was obtained.

G. Design practices that can impair consumer choice

PUBLIC FACT The Federal Trade Commission has documented dark patterns - interface and design practices that can trick or trap consumers, obscure material information, or subvert privacy and choice. The FTC has separately brought major privacy-deception enforcement actions involving Facebook. [P19-P20]

These findings provide a concrete consumer-protection pathway for testing the agency-loss theory. The investigation should identify the exact interface, statement, default, ranking choice, or omission; the traditional money or property obtained; the knowledge and intent of the actor; and every interstate transmission used to execute the transaction.

H. Social connection and mental-health harms

PUBLIC FACT The U.S. Surgeon General has warned that social media can pose profound risks to youth mental health, that evidence is insufficient to conclude it is adequately safe for children and adolescents, and that loneliness and social isolation are significant public-health threats. [P13-P15]

These findings do not prove that a platform intended to destroy families. They establish material risk, notice, and a need to compare public safety representations with internal knowledge. A criminal theory becomes stronger where internal records show that a company measured relational harm, knew a design intensified it, concealed the result, and continued the design because it increased revenue, dependency, influence, or contract value.

I. Family-formation trends: context, not attribution

PUBLIC FACT Census data show that marriage and childbearing milestones occur later and less commonly among young adults than in prior decades. CDC data show that the 2024 total fertility rate reached a record low and provisional 2025 births declined again. These trends are real; the public sources do not establish that social platforms caused them. [P21-P24]

The investigative question is narrower and testable: did any platform, funder, contractor, or government participant internally identify weakened pair-bonding, family trust, offline social coordination, or birth and marriage outcomes as an objective, a monetizable effect, or a tolerated externality? Answering that question requires internal experiments, product strategy records, content taxonomies, safety research, board materials, and causal analysis - not demographic correlation alone.

J. Public-source chronology

Period	Public-record development
1944	OSS Simple Sabotage Field Manual formalizes low-visibility organizational disruption by ordinary participants.
1979	Oracle delivers its first SQL product to the CIA, according to Computer History Museum oral history; Oracle states the U.S. Government was its first customer.
1980s	Psychological Operations in Guerrilla Warfare documents influence methods in a guerrilla setting.
1990s	Publicly funded digital-library research contributes to foundational ranking technology later associated with Google.
1999 onward	In-Q-Tel operates as a national-security technology investment channel.
2003	Palantir is founded and begins building software for the U.S. intelligence community.
2004-2005	Facebook launches; Peter Thiel becomes an early investor and board member.
2010s-2020s	Mass social graphs, ad targeting, recommendation, mobile tracking, and cross-platform identity systems scale globally.

Period	Public-record development
2023-2025	Federal public-health and consumer-protection authorities publish warnings and findings concerning social-media safety, social connection, and commercial surveillance.
2026	This referral requests preservation and an actor-by-actor criminal and regulatory inquiry.

V. ENTERPRISE STRUCTURE AND OPERATION

A. Data-to-influence cycle

Stage	Conduct to investigate
1. Collection	Acquire explicit, inferred, purchased, and observed data about identity, relationships, attention, location, interests, emotion, and vulnerability.
2. Modeling	Build profiles, social graphs, similarity groups, likelihood estimates, and predicted responses.
3. Intervention	Select content, timing, framing, frequency, social proof, notifications, and friction to move attention or action.
4. Measurement	Observe clicks, viewing time, conflict, sharing, retention, purchases, emotional reactions, and relationship effects.
5. Optimization	Update models and ranking objectives toward revenue, dependency, influence, or operational goals.
6. Concealment or disclosure	Decide what users, regulators, investors, researchers, and public customers are told about the system.

B. Means of participation

Role	Potential operation-or-management evidence
Financier or investor	Conditions tied to product direction, intelligence access, data integration, targeting, government customers, growth, engagement, or concealment; board control; approval rights; knowledge of deceptive acquisition of property.
Government customer or liaison	Requirements, tasking, evaluation, data access, domestic-use requests, waivers, feedback, procurement certifications, and direction of private capabilities.
Executive or board member	Approval of ranking objectives, experiments, risk tolerance, public statements, data practices, retention, government arrangements, and responses to warnings.
Engineer or data scientist	Knowing implementation or concealment of a fraudulent design; manipulation of metrics; bypass of controls; falsification of disclosures.
Advertiser or data intermediary	Knowing use of unlawfully or deceptively obtained data, coordinated targeting, payment for hidden influence, or concealment of source and purpose.
Counsel, compliance, or public relations	Knowing false certifications, destruction or suppression of evidence, sham disclosures, witness pressure, or obstruction; ordinary legal advice is not enough.

C. The relationship-degradation pathway

The proposed social mechanism is testable. It begins when a narrow proposition is not evaluated on its merits but routed through a preloaded group classification. The user or listener is sorted into an enemy category; symbolic content replaces the proposition; collective trauma is introduced; agreement becomes a loyalty test; and interpersonal understanding is reframed as defeat. Repetition can make the routing feel spontaneous even when the sequence is learned and externally reinforced.

The investigation should not infer criminal causation from anecdote alone. It should test the pathway against platform distribution records, recommendation exposure, ad and influencer networks, content-seeding records, coordinated accounts, experiment cohorts, message templates, moderation choices, and changes in beliefs or behavior over time.

VI. PREDICATE-OFFENSE MAPPING

A. Wire fraud - 18 U.S.C. section 1343

Wire fraud is the primary proposed predicate because the alleged system operates through electronic onboarding, consent, content transmission, advertising, billing, securities communications, contracts, subscriptions, and data transfers.

Element	Proposed proof
Scheme	Obtain money or property by materially misrepresenting or concealing how data, ranking, targeting, safety, consent, ownership, or government coordination actually operates.
Material statement or omission	A representation likely to affect a reasonable user, advertiser, investor, creator, customer, or public agency deciding whether to transfer money or property.
Intent	Internal knowledge that the representation was false or incomplete, plus purpose to obtain property through the deception.
Property object	Advertising payments, subscription revenue, public contract funds, investment capital, content or data licenses, contract rights, or other traditional property.
Interstate wire	Electronic acceptance, payment, invoice, email, app transmission, API call, investor communication, procurement submission, or cloud transfer used to execute the scheme.
Enterprise nexus	The wire furthered the Enterprise's shared objective and was not merely an isolated employee act.

Candidate wire-fraud representations to test

- The feed, recommendation, or search system is substantially user-directed or neutral when hidden objectives, interventions, or third-party tasking materially shape it.
- Consent is meaningful and informed when material collection, inference, sharing, experimentation, licensing, retention, or government access is concealed or incomprehensible.
- The service is designed primarily to connect people or serve the user when internal objectives prioritize dependency, conflict, political or operational influence, or extraction.
- Safety or well-being claims omit known internal evidence of material harm or known design choices that intensify it.
- Advertising, audience, engagement, or efficacy metrics are genuine when bots, coordinated accounts, undisclosed experiments, manipulated distribution, or misleading measurement inflate them.
- Public procurement certifications or contract deliverables accurately describe data sources, domestic use, legal compliance, model operation, or intended purpose when internal records show otherwise.

B. Mail fraud - 18 U.S.C. section 1341

The same scheme may support mail fraud where checks, paper contracts, grant records, legal notices, hardware shipments, or commercial-carrier deliveries were used to execute it. A signed check proves a payment and relationship; it becomes a fraud execution or proceeds fact only when linked to material deception, unlawful proceeds, or knowing promotion of the scheme.

C. Money laundering - 18 U.S.C. sections 1956 and 1957

Once revenue is proven to be proceeds of wire fraud, mail fraud, bribery, securities fraud, or another specified unlawful activity, transactions that knowingly promote the scheme, conceal ownership or source, or involve qualifying criminally derived property may support laundering charges. The required analysis follows the money from each proven predicate to each subsequent transaction.

D. Bribery, kickbacks, and honest-services fraud

A bribery theory requires a corrupt exchange: money, equity, employment, preferential investment access, contracts, data, or another thing of value for official action. The inquiry should examine procurement awards, regulatory treatment, intelligence access, waivers, enforcement decisions, revolving-door employment, equity grants, consulting

agreements, and undisclosed benefits. Ordinary contracting and policy agreement are not substitutes for proof of a quid pro quo or applicable statutory theory.

E. Securities and commodities fraud

Securities fraud should be examined where capital was raised or securities traded while material facts were knowingly misrepresented or concealed, including the real operation of engagement or recommendation systems, unlawful data sources, undisclosed government coordination, false user or revenue metrics, known safety liabilities, or manipulation of advertiser and investor measurements.

F. Criminal intellectual-property and trade-secret offenses

If the evidence shows willful commercial exploitation of protected works without a valid license, or knowing theft of source code, models, customer lists, confidential methods, or other trade secrets, applicable criminal copyright, economic-espionage, or trade-secret statutes may supply predicates. The investigation must distinguish actual theft from broad but legally valid contractual terms.

G. Obstruction, witness tampering, and retaliation

Obstruction predicates become available if participants destroy or alter records, falsify logs, conceal experiments after preservation duties attach, direct witnesses to lie, retaliate against whistleblowers, interfere with agency or congressional proceedings, or use sham processes to prevent lawful inquiry. The timing of deletion, litigation holds, subpoenas, complaints, warnings, and internal communications is critical.

H. Predicate summary

Potential predicate	Best evidence	Failure point to avoid
Wire fraud	Exact false statement or omission; property obtained; exact wire; knowledge and intent.	Treating generalized manipulation or loss of agency alone as property fraud.
Mail fraud	Mailing or shipment used to execute the same property fraud.	Assuming every check is fraudulent because the recipient later caused harm.
Money laundering	Specified unlawful activity proceeds; knowledge; promotion, concealment, or qualifying transaction.	Calling lawful investment or ordinary revenue laundering without a proven predicate.
Bribery / honest services	Thing of value, official or fiduciary action, corrupt exchange, concealment.	Equating access, influence, or shared ideology with bribery.
Securities fraud	Material investor deception, scienter, securities nexus.	Using social harm alone without a false securities statement.
IP / trade-secret crime	Protected subject matter, unauthorized taking/use, willfulness, economic benefit.	Treating an unfavorable but valid license as theft.
Obstruction / retaliation	Proceeding nexus, corrupt act, intent, records or witness evidence.	Treating ordinary legal defense or retention policy as obstruction.

VII. PATTERN, CONTINUITY, AND RICO COUNTS

A. Relatedness

The proposed predicates would be related if they share the same purpose - obtaining and preserving money, property, data, contracts, or institutional power through deceptive behavioral systems - and use recurring participants, victims, methods, platforms, representations, and proceeds. The schedule must show the relationship act by act rather than rely on a broad narrative.

B. Continuity

Continuity may be closed-ended if related predicates extend over a substantial period, or open-ended if they are a regular way of conducting an ongoing enterprise or threaten repetition. Recurring onboarding representations, ad

transactions, subscription renewals, procurement certifications, securities communications, and concealment could establish continuity when their criminal elements are proven.

C. Proposed RICO counts

Count	Statute	Proposed theory
Count One	18 U.S.C. section 1962(d)	Agreement to conduct or participate in the affairs of the Enterprise through a continuing pattern of qualifying fraud, laundering, bribery, IP crime, or obstruction.
Count Two	18 U.S.C. section 1962(c)	Named persons operated or managed the Enterprise through related and continuous predicate acts.
Count Three	18 U.S.C. section 1962(a)	Income derived from proven racketeering activity was used or invested to acquire, establish, or operate the Enterprise.
Counts Four-XX	18 U.S.C. sections 1341, 1343, 1348, 1956, 1957, 1503, 1510, 1512, 1513, and other applicable predicates	Transaction-specific substantive counts supported by exact actors, dates, communications, property, intent, and nexus.

D. Illustrative pattern theory

The proposed pattern is not simply that technology companies collect data or that social media creates conflict. The proposed pattern is repeated property fraud and related offenses in which participants knowingly concealed the true operation, purpose, risks, data use, coordination, or metrics of behavioral systems to obtain property; used proceeds and institutional relationships to expand the systems; and obstructed accountability. Family and relationship degradation is relevant as a measured or foreseeable fruit of the pattern and as evidence bearing on materiality, intent, notice, and damages.

VIII. EVIDENCE MATRIX AND INVESTIGATIVE PLAN

A. Evidence matrix

Issue	Public evidence now	Compulsory evidence needed
Enterprise purpose	Funding, governance, customer, product, and doctrine relationships.	Internal statements of purpose; strategy; tasking; board records; cross-entity communications; knowledge of harmful objectives.
Wire fraud	Public claims, consent interfaces, privacy policies, product descriptions, regulatory findings.	Versioned disclosures; internal contradiction; exact transactions; property transfer; scienter; decision-makers.
Behavioral influence	Manuals, public research, platform design, recommendation functions, downstream examples.	Experiment registries; exposure data; targeting instructions; coordinated campaigns; source attribution; intervention goals.
Family and social harm	Public-health warnings, research, complaints, anecdotal downstream evidence.	Product-specific internal studies; measured relationship outcomes; risk reviews; executive decisions; profit or operational benefit.
Government role	Public investment, contracts, technology lineage, agency publications.	Tasking, classified and unclassified procurement, liaison records, legal approvals, minimization, domestic-use restrictions, oversight findings.
Obstruction	Whistleblower accounts, gaps, deletion events, inconsistent public explanations where authenticated.	Litigation holds, deletion logs, witness communications, retaliation files, privilege review, altered reports, subpoena responses.

B. First 90-day investigative plan

Period	Actions
Days 1-10	Conflict screen; preservation; identify custodians; freeze automated deletion; obtain public filings, contracts, policies, interface versions, and known complaints.
Days 11-30	Issue subpoenas and voluntary requests; interview former employees and whistleblowers; collect investment, procurement, board, ranking, experiment, safety, and data-flow records.
Days 31-60	Build actor and transaction databases; reconstruct exact wires and mails; compare public statements with internal knowledge; trace proceeds; identify possible obstruction.
Days 61-90	Test enterprise, agreement, operation-or-management, predicates, relatedness, and continuity; prepare declination, expansion, civil referral, or grand-jury recommendation.

C. Expert disciplines

- Digital forensics and version-control reconstruction.
- Recommendation-system, machine-learning, ad-tech, and social-graph engineering.
- Behavioral science, propaganda, influence operations, and information warfare.
- Consumer protection, privacy, contract, securities, procurement, and public-corruption law.
- Causal inference, epidemiology, social-network analysis, and mental-health research.
- Forensic accounting, money tracing, valuation, and damages.
- First Amendment, intelligence law, domestic-operations safeguards, classification, and oversight.

D. Causation protocol

Causation should be tested at four layers: (1) exposure - what content or design the person encountered; (2) routing - what recommendation, ad, network, or coordinated source delivered it; (3) mechanism - what belief, category, emotion, or behavior changed; and (4) outcome - what measurable economic, health, civic, or relational consequence followed. No single layer substitutes for the others.

IX. ANTICIPATED DEFENSES AND SPECIAL PROBLEMS

Expected defense	Investigative response
No common purpose; independent lawful businesses.	Test shared tasking, funding conditions, board overlap, communications, coordinated deployment, and reciprocal benefit. Do not infer agreement solely from overlap.
No traditional property object.	Identify exact money, contracts, licenses, content rights, public funds, investment capital, or trade secrets obtained by deception; apply Ciminelli and Kousisis.
Algorithms are neutral tools and users choose content.	Examine objective functions, interventions, experiments, ranking controls, dark patterns, target selection, and hidden operational requirements.
First Amendment and editorial discretion.	Separate protected speech and editorial choices from fraud, bribery, theft, laundering, unlawful surveillance, false certifications, and obstruction.
Government authorization or national security.	Demand legal authority, scope, minimization, domestic-use safeguards, oversight, necessity, and whether private monetization exceeded authorization.
Public disclosures defeated materiality.	Compare clarity, timing, prominence, completeness, audience understanding, internal knowledge, and whether later disclosures cured earlier property transfers.
Social harm is speculative or multifactorial.	Use product-specific experiments, exposure data, internal studies, temporal analysis, control groups, and alternative-cause testing.
Investment and contracts prove only ordinary commerce.	Agree unless evidence connects them to knowing fraudulent or corrupt objectives; trace conditions, reporting, tasking, and proceeds.
No operation or management by peripheral actors.	Charge only participants shown to direct enterprise affairs; distinguish ordinary services from knowing managerial participation.
Statute of limitations and venue.	Identify timely predicates, continuing conduct, concealment, exact wires, victims, districts, and proceeds transactions.

Special problem: attribution

A downstream script can match documented influence architecture without proving who authored, seeded, funded, ranked, or amplified it. Attribution requires platform records, creator and payment records, coordinated-account evidence, network analysis, government or contractor tasking, and authenticated communications. The investigation must not replace attribution evidence with similarity alone.

Special problem: lawful persuasion versus criminal deception

Persuasion, ideology, advertising, advocacy, and even polarizing speech are generally not crimes. The criminal line is crossed by independently unlawful means: material property fraud, bribery, theft, laundering, unlawful surveillance, false procurement or securities statements, obstruction, or another qualifying predicate. This memorandum targets those means, not viewpoint or disagreement.

X. PROPOSED DRAFT CHARGING FRAMEWORK

DRAFTING NOTICE

The following is a charging template modeled on the structure of a federal RICO submission. It is not an indictment and deliberately uses placeholders where the public record does not supply a provable actor, date, statement, property transfer, or intent.

COUNT ONE - RICO CONSPIRACY

1. From at least [START DATE] through [END DATE / PRESENT], in [DISTRICT] and elsewhere, the defendants [NAMES], being persons associated with the Behavioral Dependency and Commercial Surveillance Enterprise, knowingly and intentionally conspired with each other and with others known and unknown to violate 18 U.S.C. section 1962(c), in violation of 18 U.S.C. section 1962(d).
2. The Enterprise was an association-in-fact whose members functioned as a continuing unit with the common purpose of obtaining and preserving money, property, data, contracts, licenses, and institutional power through materially deceptive behavioral-influence and commercial-surveillance systems, and of protecting and expanding those systems through coordinated financing, procurement, distribution, concealment, and reinvestment.
3. The defendants agreed that members of the Enterprise would commit at least two acts of racketeering activity, including wire fraud, mail fraud, money laundering, bribery, securities fraud, intellectual-property offenses, obstruction, and witness retaliation, as specified in the racketeering-act schedule.

COUNT TWO - SUBSTANTIVE RICO

4. The allegations of paragraphs 1 through 3 are realleged.
5. Each named defendant was employed by or associated with the Enterprise and knowingly conducted or participated, directly or indirectly, in the conduct of its affairs through a pattern of racketeering activity, in violation of 18 U.S.C. section 1962(c).
6. The pattern consisted of the related and continuous racketeering acts set forth in Schedule A, which shared common purposes, participants, victims, methods, results, and proceeds and were a regular way of conducting the Enterprise's affairs or threatened continued repetition.

COUNT THREE - INVESTMENT OF RACKETEERING INCOME

7. The allegations of paragraphs 1 through 6 are realleged.

8. After receiving income derived, directly or indirectly, from a pattern of racketeering activity, the defendants used or invested part of that income in the acquisition, establishment, or operation of the Enterprise, in violation of 18 U.S.C. section 1962(a).

ILLUSTRATIVE WIRE-FRAUD COUNT

9. On or about [DATE], in [DISTRICT] and elsewhere, defendant [NAME], for the purpose of executing the scheme described above, knowingly caused to be transmitted by means of interstate wire communication [DESCRIPTION OF EMAIL / APP TRANSMISSION / PAYMENT / CONSENT / PROCUREMENT SUBMISSION], containing or executing the material representation or omission that [EXACT LANGUAGE OR CONDUCT], thereby obtaining [IDENTIFIED MONEY OR PROPERTY] from [VICTIM / PAYOR], in violation of 18 U.S.C. section 1343.

Schedule A - racketeering act pleading fields

Field	Required allegation and proof
Act number	RA-__
Date and district	[Exact date, origin, destination, venue]
Actor and role	[Named person; enterprise function; operation-or-management facts]
Predicate statute	[Section 1341, 1343, 1348, 1956, 1957, 1512, etc.]
False statement or prohibited act	[Exact representation, omission, transfer, bribe, theft, concealment, or obstruction]
Victim / recipient	[User, advertiser, investor, creator, agency, customer, witness]
Property or proceeding	[Exact money/property or proceeding affected]
Knowledge and intent	[Internal record, testimony, warning, directive, concealment]
Enterprise nexus	[How the act conducted or protected enterprise affairs]
Relatedness and continuity	[Common purpose, participants, method, result, repetition]

Forfeiture allegation

Upon conviction, the government should seek forfeiture only of property authorized by statute and traceable to the offense, including interests acquired or maintained in violation of Section 1962, proceeds obtained from racketeering activity, and substitute assets where legally available. A forensic tracing schedule should separate lawful enterprise value from criminal proceeds and tainted interests.

XI. CONCLUSION AND SIGNATURE

The public record establishes enough to require a serious, conflict-screened investigation. It establishes documented influence and sabotage doctrine; durable intelligence-technology-capital relationships; mass data and social-graph infrastructure; commercial-surveillance findings; public-health warnings; and a plausible mechanism through which preloaded identity scripts can displace direct human understanding.

The public record does not, standing alone, prove the internal agreement, material deception, property object, actor-level intent, or exact predicate acts required for conviction. Those are not reasons to dismiss the matter. They are the reason compulsory process exists. The question is no longer whether the architecture could exist. The question is who designed, funded, directed, represented, profited from, measured, protected, and concealed each material part of it.

Accordingly, the undersigned requests immediate preservation, independent investigation, grand-jury review where warranted, and referral of all proven criminal, civil, administrative, and oversight violations to the competent authority.

SUBMITTED BY BJ Klock

SIGNATURE _____

DATE August 5, 2026

CONTACT _____

LOCATION Connecticut, United States

APPENDIX A. PUBLIC-SAFE DOWNSTREAM MECHANISM

PUBLIC EDITION PRIVACY RULE

An originating private interpersonal exchange prompted the downstream inquiry. The exchange, screenshots, direct quotations, timestamps, and identifying context are intentionally withheld from this public edition. The underlying materials are preserved separately. Withholding them prevents a public-interest referral from becoming a public trial of a nonpublic person.

EVIDENTIARY LIMIT

This appendix describes a hypothesis-generating mechanism only. It does not establish platform attribution, institutional authorship, coordination, criminal intent, or population-level causation.

Observed routing model



A. MECHANISM DEFINITIONS

The definitions below are prospective coding categories. They describe what an investigator would look for in independently sampled material; they are not findings about any named person, platform, or institution.

Mechanism	Operational definition	Evidence required
Proposition displacement	The original claim is no longer evaluated on its own terms.	Full chronology showing when and how the subject changed.
Identity classification	The speaker is assigned to a hostile group or treated as its representative.	Exact language, sequence, and surrounding context.
Symbolic substitution	A slogan, meme, or hypothetical replaces the original proposition.	Exposure history, source, routing, and repetition data.
Scope escalation	An individual event expands into collective danger, trauma, or historical grievance.	Temporal ordering and the relevance of each introduced issue.
Loyalty enforcement	A demanded answer is used to classify allegiance rather than test the proposition.	Exact demand, allowed answers, and interpersonal consequences.
Reopening after closure	A settled topic is reintroduced through the approved symbolic frame.	Boundary request, acknowledgment, and later reopening.
Winner-loser resolution	Understanding is treated as defeat, surrender, or loss of status.	Language used to end the exchange and reported outcome.
Intimate-channel transmission	A learned frame operates inside a close relationship or trusted group.	Privacy-protected evidence and consent or lawful authority to review.

The categories must be pre-registered and applied equally to supportive, contradictory, and null examples. Similarity to a known influence method is not attribution evidence by itself.

B. INVESTIGATIVE RELEVANCE

The public-interest question is not whether an ordinary person consciously participates in an operation. The question is whether platforms, funders, contractors, or public actors designed, seeded, ranked, measured, exploited, or concealed a repeatable routing architecture. Once a frame is widely distributed and socially rewarded, ordinary people can reproduce it without knowing its origin.

C. Four-layer causation test

1. Exposure	What content, interface, experiment, or repeated frame did the person encounter?
2. Routing	What recommendation, ad, network, influencer, coordinated source, or product decision delivered it?
3. Mechanism	What category, belief, emotion, salience, or behavior changed, and by what measurable process?
4. Outcome	What economic, health, civic, relational, or behavioral consequence followed?

D. Evidence required before attribution

Attribution requires more than resemblance. Investigators should obtain platform exposure and recommendation records; creator, advertiser, and payment records; coordinated-account evidence; experiment assignments; content-seeding instructions; model and ranking changes; government or contractor tasking; authenticated communications; and appropriate control data.

E. Falsification conditions

THIS IS THE TEST

The theory must be narrowed or rejected where: (1) comparable routing appears at similar rates without relevant exposure or reinforcement; (2) platform and internal records show no relevant seeding, ranking, optimization, measurement, or knowledge; (3) alternative causes explain the observed sequence better; (4) the alleged actor made no material misrepresentation, obtained no traditional property through deception, and committed no qualifying predicate; or (5) independent replication fails under pre-registered methods.

A private example may generate a question. It cannot answer the question. The answer must come from replicated evidence and the internal records held by the relevant custodians.

APPENDIX B. REPLICATION AND FALSIFICATION PROTOCOL

This protocol converts the downstream mechanism into a researchable, privacy-protective test. It is designed to prevent a selected private exchange from carrying more evidentiary weight than it can support.

Required protocol

1. Pre-register the mechanism definitions, hypotheses, exclusions, scoring rules, and falsification criteria.
2. Remove names and identifying details; obtain consent or another lawful basis before reviewing private material.
3. Sample conversations independently rather than selecting only high-conflict examples.
4. Use at least two blinded raters and report inter-rater agreement and disagreements.
5. Separate direct transcript facts from inferred meaning and causal interpretation.
6. Collect exposure and routing histories before making source or platform attribution claims.
7. Compare against matched control conversations and test plausible alternative causes.
8. Report null, contradictory, and adverse findings rather than retaining only supportive examples.
9. Do not translate a mechanism score into authorship, government involvement, criminal intent, or a RICO predicate.
10. Preserve source integrity, chain of custody, access logs, and the legal basis for collection.

Permitted and prohibited conclusions

Permitted when supported	Not permitted without additional proof
Frequency of a defined conversational sequence in the sampled material.	That a named actor authored, seeded, or funded the sequence.
Association between verified exposure and a measured routing outcome.	That a government agency directed a private conversation.
Replication or non-replication under the pre-registered protocol.	That resemblance establishes coordination or criminal intent.
A focused basis for preservation, interviews, or compulsory records.	That a mechanism alone satisfies any RICO predicate or proves population causation.

RESTRICTED ANNEX HANDLING

Any private source material should remain in a separately controlled evidentiary annex with access limits, chain-of-custody records, and no public distribution.

APPENDIX C. PREDICATE ACT SCHEDULE TEMPLATE

This schedule converts a broad theory into admissible, transaction-specific proof. One row should be completed for each alleged predicate. A row should not be scored as chargeable until every mandatory field is supported by evidence.

Act	Date	Actor	Predicate	Execution	Property / proceeding	Scienter	Enterprise nexus
RA-01	[Date]	[Actor]	[Statute]	[Wire/mail/act]	[Property/proceeding]	[Intent proof]	[Nexus]
RA-02	[Date]	[Actor]	[Statute]	[Wire/mail/act]	[Property/proceeding]	[Intent proof]	[Nexus]
RA-03	[Date]	[Actor]	[Statute]	[Wire/mail/act]	[Property/proceeding]	[Intent proof]	[Nexus]
RA-04	[Date]	[Actor]	[Statute]	[Wire/mail/act]	[Property/proceeding]	[Intent proof]	[Nexus]
RA-05	[Date]	[Actor]	[Statute]	[Wire/mail/act]	[Property/proceeding]	[Intent proof]	[Nexus]
RA-06	[Date]	[Actor]	[Statute]	[Wire/mail/act]	[Property/proceeding]	[Intent proof]	[Nexus]
RA-07	[Date]	[Actor]	[Statute]	[Wire/mail/act]	[Property/proceeding]	[Intent proof]	[Nexus]
RA-08	[Date]	[Actor]	[Statute]	[Wire/mail/act]	[Property/proceeding]	[Intent proof]	[Nexus]
RA-09	[Date]	[Actor]	[Statute]	[Wire/mail/act]	[Property/proceeding]	[Intent proof]	[Nexus]
RA-10	[Date]	[Actor]	[Statute]	[Wire/mail/act]	[Property/proceeding]	[Intent proof]	[Nexus]

Mandatory supporting file for each act

- Authenticated communication, transaction, mailing, wire, payment, filing, code event, or witness act.
- Exact representation or prohibited conduct and why it was false or unlawful when made.
- Identified victim or recipient and the traditional property or proceeding affected.
- Evidence of knowledge and intent, including warnings, contradictions, concealment, directives, or admissions.
- Evidence that the actor operated or managed enterprise affairs or knowingly agreed to facilitate the RICO endeavor.
- Relatedness and continuity facts connecting the act to the alleged pattern.
- Venue, limitations, privilege, classification, admissibility, and chain-of-custody analysis.

APPENDIX D. PRESERVATION AND PRODUCTION CATEGORIES

Category	Preserve and produce
Governance	Board and committee materials; investor rights; cap tables; voting arrangements; founder-control instruments; strategy and risk presentations.
Government relationships	Contracts, grants, procurement files, task orders, statements of work, clearances, liaison records, legal approvals, minimization rules, audits, and technology-transfer records.
Product and ranking	Source code, repositories, feature flags, model versions, objective functions, ranking weights, recommender changes, safety filters, suppression and amplification rules.
Experiments	A/B tests, cohort assignments, hypotheses, outcome measures, experiment registries, unpublished results, adverse findings, ethics and legal reviews.
Data	Schemas, dictionaries, identity resolution, social graphs, inferred attributes, data-broker purchases, third-party sharing, retention, deletion, model training, government access.
Content operations	Seed accounts, coordinated campaigns, influencer payments, moderation instructions, policy exceptions, trend interventions, content whitelists and blacklists.
Commercial representations	Terms, consent flows, privacy notices, safety claims, ad claims, metric definitions, investor disclosures, procurement certifications, customer representations.
Money and property	Checks, wires, invoices, subscriptions, ad payments, public funds, licensing, content rights, proceeds transfers, reinvestment, concealment, and beneficial ownership.
Warnings and harms	Complaints, research, internal studies, relationship and family metrics, mental-health findings, child-safety findings, escalation records, executive responses.
Oversight and concealment	Regulator responses, subpoena productions, congressional responses, deletion logs, litigation holds, witness communications, retaliation, non-disclosure agreements.

Suggested preservation language

You are directed to preserve all documents, electronically stored information, source code, model artifacts, communications, transaction records, logs, metadata, and physical records potentially relevant to the subjects and categories in this referral. Preservation includes active systems, archives, personal devices used for business, ephemeral messaging, collaboration tools, deleted-item repositories, backups, code histories, experiment platforms, vendor systems, and records held by agents or contractors. Suspend routine destruction and document every preservation step, custodian, exception, and loss.

APPENDIX E. AUTHORITIES AND PUBLIC SOURCES

The sources below are primary or official public records used to structure this draft. Links are included for verification. Access dates should be updated on filing.

- [L1] 18 U.S.C. sections 1961-1968, Racketeer Influenced and Corrupt Organizations. [Official source](#)
- [L2] U.S. Department of Justice, Justice Manual 9-110.000, Organized Crime and Racketeering. [Official source](#)
- [L3] U.S. Department of Justice, RICO Prosecution Memorandum - Statement of the Law. [Official source](#)
- [L4] 18 U.S.C. section 1341, Frauds and swindles. [Official source](#)
- [L5] 18 U.S.C. section 1343, Fraud by wire, radio, or television. [Official source](#)
- [L6] Ciminelli v. United States, 598 U.S. 306 (2023). [Official source](#)
- [L7] Kousisis v. United States, 605 U.S. ____ (2025). [Official source](#)
- [L8] U.S. Department of Justice, Criminal RICO: A Manual for Federal Prosecutors. [Official source](#)
- [L9] 18 U.S.C. sections 1956-1957, Money laundering and criminally derived property transactions. [Official source](#)
- [L10] 18 U.S.C. Chapter 73, Obstruction of Justice. [Official source](#)
- [P1] Central Intelligence Agency Reading Room, Psychological Operations in Guerrilla Warfare. [Official source](#)
- [P2] Central Intelligence Agency, The Art of Simple Sabotage. [Official source](#)
- [P3] Office of Strategic Services, Simple Sabotage Field Manual, CIA-hosted copy. [Official source](#)
- [P4] In-Q-Tel, official history: established by the CIA in 1999 as a strategic investment firm. [Official source](#)
- [P5] In-Q-Tel, official milestones describing its CIA technology-investment mission. [Official source](#)
- [P6] Palantir Technologies Inc., 2020 Form S-1 describing its start building software for the U.S. intelligence community. [Official source](#)
- [P7] Facebook, Inc., 2012 Form S-1 identifying Peter Thiel as an early investor and director since April 2005. [Official source](#)
- [P8] Palantir Technologies 2020 Form S-1 identifying Peter Thiel among its founders and founder voting structure. [Official source](#)
- [P9] National Science Foundation, On the Origins of Google. [Official source](#)
- [P10] Federal Trade Commission, A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services. [Official source](#)
- [P11] Federal Trade Commission staff report PDF on social-media and video-streaming data practices. [Official source](#)
- [P12] Federal Trade Commission press release summarizing findings of vast surveillance and inadequate controls. [Official source](#)
- [P13] U.S. Surgeon General, Social Media and Youth Mental Health Advisory. [Official source](#)
- [P14] U.S. Surgeon General, Our Epidemic of Loneliness and Isolation Advisory. [Official source](#)
- [P15] U.S. Department of Health and Human Services, Social Connection resources. [Official source](#)
- [P16] In-Q-Tel, About: official statement that the CIA established IQT in 1999. [Official source](#)
- [P17] Oracle, U.S. Defense and Intelligence: official statement that the U.S. Government was Oracle's first customer. [Official source](#)
- [P18] Computer History Museum, RDBMS Workshop: Oracle - first product delivered to the CIA in 1979 and the Oracle project-name account. [Official source](#)
- [P19] Federal Trade Commission, Bringing Dark Patterns to Light. [Official source](#)
- [P20] Federal Trade Commission, 2019 Facebook privacy enforcement action and \$5 billion penalty. [Official source](#)
- [P21] U.S. Census Bureau, Most Young Adults Had Not Reached Key Milestones of Adulthood in 2024. [Official source](#)
- [P22] U.S. Census Bureau, 2025 estimates on families and living arrangements, including median age at first marriage. [Official source](#)

[P23] CDC/NCHS, Births: Final Data for 2024 - record-low total fertility rate. [Official source](#)

[P24] CDC/NCHS, Births: Provisional Data for 2025. [Official source](#)

Selected controlling authorities for a final filing

- Boyle v. United States, 556 U.S. 938 (2009) - association-in-fact structure.
- Reves v. Ernst & Young, 507 U.S. 170 (1993) - operation or management.
- H.J. Inc. v. Northwestern Bell Telephone Co., 492 U.S. 229 (1989) - relatedness and continuity.
- Salinas v. United States, 522 U.S. 52 (1997) - RICO conspiracy.
- United States v. Turkette, 452 U.S. 576 (1981) - enterprise and pattern proof.
- Sedima, S.P.R.L. v. Imrex Co., 473 U.S. 479 (1985) - elements and civil RICO principles.

FINAL FILING REQUIREMENT

Before submission as an accusation against any named person, replace every placeholder with authenticated evidence, add circuit-specific law, resolve privilege and classification issues, obtain qualified counsel review, and distinguish prosecutable facts from political or moral conclusions.