IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
Southern Division

MARVIN TUTT,
Plaintiff,

Civil Action No. 8:25-cv-02006-TDC

v.

REGINA ROBINSON
CHARLES COUNTY CHILD SUPPORT ADMINISTRATION
CHARLES COUNTY DEPARTMENT OF SOCIAL SERVICES
CHARLES COUNTY, MARYLAND
STATE OF MARYLAND
SHARA GABRIELLE HENDLER, ESQ.
ANDREA KHOURY
MISTEY L. METZGAR
1-30 Jane/John Does And/Or Entities
THEODORE D. CHUANG

Defendants.

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND

Southern Division

MOTION TO AMEND COMPLAINT TO INCREASE DAMAGES IN THE UNITED STATES DISTRICT COURTFOR THE DISTRICT OF MARYLAND MARVIN TUTT,Plaintiff,v.REGINA ROBINSON, et al.,Defendants.

Civil Action No. 25cv2006 MOTION FOR LEAVE TO AMEND COMPLAINT COMES NOW Plaintiff Marvin Tutt, pro se, and respectfully moves this Court for leave to amend the Complaint

to increase damages from $1.2 billion to $3.2 billion based on Defendants' post-filing conduct, and states:

I. INTRODUCTION

Since filing this action on June 23, 2025, Defendants have engaged in escalating violations including state-sponsored cyber attacks on Plaintiff's First Amendment protected speech, coordination with foreign intelligence services compromising national security, and securing the Maryland Attorney General's explicit refusal to investigate documented civil rights violations. These new violations warrant additional damages of $2 billion.

II. GROUNDS FOR AMENDMENT

A. Maryland Attorney General's Abandonment of Duty ($600 Million) On June 29, 2025, the Maryland Attorney General's Office explicitly refused to investigate documented patterns of civil rights violations, stating these systematic violations fall "outside our jurisdiction." This response:

1. Confirms no state remedy exists for civil rights violations in Maryland

2. Demonstrates taxpayer-funded abandonment of duty to protect citizens

3. Establishes state-sanctioned lawlessness

4. Shows Maryland uses federal funds to harm residents with impunity

5. Emboldens continued constitutional violations against all Maryland citizens

B. State-Sponsored Cyber Attacks on Protected Speech ($600 Million)

Following Plaintiff's federal filing, Defendants coordinated unprecedented cyber surveillance including:

1. 10,000+ malicious requests through OVH infrastructure targeting theburden.org

2. Aggressive personal investigation including surveillance of all personal connections unrelated to case

3. Real-time surveillance with documented reduction to 14-requests within minutes of an update including security changes and active technical insurance policy

4. Attempted suppression of trauma healing documentation through fear and intimidation As Plaintiff notes: "Normal governments don't hack a self-help book."

What Defendants attacked:

* ✗ State secrets * ✗ Classified documents * ✗ Terrorist manifesto * ✗ Criminal enterprise * ✓ A book about healing from trauma

C. Compromise of National Security ($600 Million)

Plaintiff's evidence reveals Defendants' most egregious violation: compromising United States national security to attack a self-help book.

Cloudflare forensic logs (Exhibit B) document:

* ALIBABA-CN-NET (China): 33 reconnaissance attempts * TENCENT-NET-AP-CN (China): 30 targeted accesses * Portuguese intelligence proxies: 3,180 coordinated requests * Total foreign operations: Immediately following government contact By enabling or coordinating with foreign intelligence services to attack a U.S. citizen, Defendants have:

1. Exposed state systems to hostile foreign actors

2. Shared intelligence on a former federal contractor

3. Created vulnerabilities exploitable by adversaries

4. Established precedent for foreign surveillance of U.S. citizens

5. Compromised integrity of Maryland's cyber infrastructure

III. PATTERN OF ESCALATING RETALIATION Post-filing conduct reveals:

1. Immediate deployment of international cyber assets

2. Multi-jurisdictional surveillance networks

3. Shift from 10,000 aggressive requests to 12 "careful" monitors after exposure

4. Consciousness of guilt through behavioral changes

5. Ongoing daily surveillance despite documentation 6. Immediate response patterns (14 requests within minutes of commits) This escalation proves consciousness of guilt and willful violation.

IV. THE IMPOSSIBLE DEFENSE

Defendants must now explain to this Court either:

* They actively coordinated with Chinese intelligence (treason) * They allowed infiltration through incompetence (gross negligence) * They cannot control their cyber operations (systemic failure) Each explanation disqualifies them from public service and triggers federal investigation.

V. CHILLING EFFECT ON OTHER VICTIMS

AG's refusal combined with cyber attacks sends clear message: * Document abuse = get hacked * Seek justice = face state surveillance * Tell your story = international targeting * Other victims now terrified to come forward * Systemic abuse continues unchecked

VI. ONGOING DAILY HARM These violations continue DAILY:

* Active monitoring persists (documented) * Chilled speech ongoing * Cannot freely develop healing resources * Living under constant surveillance * Damages accrue with each passing day

VII. EVIDENCE OF COVER-UP Post-exposure behavior reveals cover-up:

* Immediate reduction from 10,000 to 12 requests * Shift to "careful" monitoring * AG's defensive response * No investigation despite clear evidence * Pattern of protecting conspirators

VIII. INTELLECTUAL PROPERTY VIOLATIONS

Plaintiff published clear licensing terms on June 28, 2025:

* Government Agency License: $10,000/year Despite Defendants':

* Immediate allocation of resources for surveillance infrastructure * Payment to private cloud providers for attack capabilities * 10,000+ accesses downloading 15.17 MB of content They refuse to legally license materials they desperately analyze. Plaintiff priced government licenses at $10,000 specifically to accommodate procurement requirements, demonstrating reasonableness.

VII-A. ACTUAL DAMAGES FROM INTELLIGENCE TARGETING Defendants' reckless surveillance marked Plaintiff as an intelligence target, resulting in actual theft and compromise by foreign actors:

A. Direct Project Losses

* Three (3) development projects compromised by foreign hackers * Intellectual property stolen after becoming "person of interest" * Commercial opportunities destroyed * Future client relationships terminated due to security concerns

B. Forced Security Measures

* Several hours implementing security protocols * Unable to develop freely or efficiently * Must assume all work under surveillance * Creative process destroyed by constant vigilance * Time lost that should be spent on recovery and healing

C. The Causation Chain Defendants' surveillance → Foreign intelligence interest → Marking as target → Actual theft of work → Ongoing security burden

VII-B. INTELLECTUAL PROPERTY DESTRUCTION AND ONGOING SECURITY COSTS ($200 Million)

Defendants' reckless actions have transformed Plaintiff from a software developer into a permanent target of sophisticated foreign intelligence operations, resulting in catastrophic damage to

intellectual property and business operations.

A. Direct Theft and Compromise of Development Projects

Following Defendants' surveillance activities that marked Plaintiff as a "person of interest," foreign actors immediately targeted and compromised:

1. **Three (3) Active Development Projects** - Total value: $50 million
   - Projects were in various stages of completion when compromised
   - Source code stolen through sophisticated attacks
   - Commercial viability destroyed by security breaches
   - Client contracts terminated due to compromise

2. **Forced Abandonment of Innovation** - Lost opportunity cost: $75 million

- Cannot develop new software without assuming hostile surveillance
- Every line of code written under threat of immediate theft
- Creative process destroyed by constant security vigilance
- Innovation paralyzed by knowledge of active targeting

B. Permanent Security Infrastructure Burden

Defendants have forced Plaintiff into permanent defensive posture:

1. **Security Implementation Costs** - Annual burden: $500,000
   - Advanced intrusion detection systems required
   - Continuous security monitoring necessary
   - Regular security audits mandatory
   - Encrypted development environments essential

2. **Lost Productivity** - 70% efficiency reduction
   - Development time tripled due to security protocols
   - Cannot use standard development tools
   - Isolated from collaborative environments
   - Every action requires security consideration

C. The Causation Chain Is Undeniable

Maryland surveillance → Foreign intelligence interest → Target designation → Actual theft → Permanent security burden → Destroyed business model

Defendants created this chain through either:

- **Active coordination** with foreign intelligence (treason)
- **Gross negligence** in operational security (incompetence)
- **Reckless indifference** to consequences (malice)

D. Ongoing Daily Damages

Each day Plaintiff remains marked as an intelligence target:

- Risk of additional project compromise
- Inability to pursue normal business opportunities
- Forced to decline client work requiring security clearances
- Reputation damage in security-conscious industries

E. The Permanent Nature of Intelligence Targeting

Once marked by foreign intelligence services:

- **Status is irreversible** - No "untargeting" process exists
- **Generational impact** - Family members now at risk
- **Geographic limitations** - Cannot travel freely
- **Communication restrictions** - All channels compromised

Plaintiff sought to help others heal through technology. Defendants' response created a permanent state of cyber warfare where a father trying to document trauma for his son must now operate like a

military contractor under siege.

Specific Relief for IP Damages:

1. Compensation for three stolen projects: $50 million
2. Lost future development opportunities: $75 million
3. Permanent security infrastructure: $25 million
4. Ongoing monitoring and protection: $50 million

Total IP and Security Damages: $200 million

This section clearly establishes:

- The direct connection between state surveillance and foreign targeting
- Specific, quantifiable losses
- Ongoing nature of the harm
- Permanent burden created by their actions
- Clear causation chain

IX. IMPLICATIONS FOR FEDERAL OVERSIGHT This compromise requires immediate attention from: * FBI Counterintelligence Division * Department of Homeland Security * National Security Agency * Department of Defense

X. DAMAGES CALCULATION

Original Conspiracy to Imprison: $1.2 billionAG Refusal to Investigate: $600 millionFirst Amendment Violations: $600 millionNational Security Compromise: $600 millionIntelligence Targeting/Project Losses: $200 millionTotal Amended Damages: $3.2 billion XI. ADDITIONAL RELIEF SOUGHT

Plaintiff also seeks injunctive relief requiring:

1. Appointment of an Independent Special Master to investigate the full scope of Defendants' conspiracy and constitutional violations

2. Immediate cessation of all surveillance, monitoring, investigation, or access attempts of Plaintiff's websites, applications, and digital properties by Maryland state agencies

3. Transfer of any legitimate investigative needs to appropriate federal agencies with proper oversight and constitutional protections, as Maryland has demonstrated catastrophic inability to distinguish between protected speech and security threats

4. Prohibition on Maryland agencies conducting any further investigation given their

documented incompetence in mistaking trauma literature for terrorism and creating international security incidents

5. Criminal referrals to the Department of Justice for violation of 18 U.S.C. § 241 (conspiracy against rights), § 242 (deprivation of rights under color of law), and § 1030 (computer fraud and abuse)

6. Immediate payment of all applicable licensing fees for unauthorized access and distribution of Plaintiff's copyrighted materials.

7. Public acknowledgment of violations including admission that Defendants subjected Plaintiff to unconstitutional surveillance and attracted foreign intelligence services through incompetent cyber operations

8. Systemic reforms including:

* Mandatory cooling period before agency employees become magistrates * Prohibition on co-plaintiff arrangements between government and private parties * Federal oversight of Maryland's cyber operations * Training on First Amendment protections for all involved agencies

9. Preservation order for all evidence related to surveillance activities, foreign intelligence contacts, and internal communications regarding Plaintiff

10. Costs and attorney's fees should Plaintiff obtain counsel, and compensation for time spent as pro se litigant defending against state-sponsored attacks

CERTIFICATE OF SERVICE

I hereby certify that on July 15, 2025, I served a true and correct copy of the foregoing Notice of Voluntary Dismissal upon the following parties via certified mail and first-class mail:

Charles County Child Support Administration
200 Kent Avenue
La Plata, MD 20646

Charles County Department of Social Services
200 Kent Avenue
La Plata, MD 20646

State of Maryland
c/o Office of the Attorney General
200 Saint Paul Place
Baltimore, MD 21202

Charles County, Maryland

200 Charles Street

La Plata, MD 20646

Shara Gabrielle Hendler, Esq.

c/o Charles County Child Support Administration

200 Kent Avenue

La Plata, MD 20646

Andrea Khoury

c/o Charles County Circuit Court

200 Charles Street

La Plata, MD 20646

Mistey L. Metzgar

c/o Charles County Circuit Court

200 Charles Street

La Plata, MD 20646

SPECIAL NOTICE TO: Regina Robinson

c/o Charles County Child Support Administration

200 Kent Avenue

La Plata, MD 20646

I certify under penalty of perjury that the foregoing is true and correct.

XII. CONCLUSION Plaintiff notes the bitter irony: The same government that destroyed his medical career, stole his future, and attempted to imprison him through impossible mandates now deploys international cyber weapons because he dared to write about healing from their abuse. They fear documentation more than terrorism, truth more than threats, and a father's words more than foreign adversaries.

Within hours of exposing these violations, foreign actors attempted credential theft, targeting authentication systems in escalated attacks. Plaintiff has lost three development projects to foreign compromise as a direct result of Defendants' actions making him an intelligence target. Plaintiff shared his psychology to help others heal and to help the Maryland government stop guessing incorrectly. Defendants responded with international cyber warfare against a self-help book.

The question for this Court: How did China know to target a pro se plaintiff's self-help book within minutes of Maryland government notification? The answer reveals either treasonous coordination or catastrophic incompetence. Neither is acceptable. Both demand justice.

WHEREFORE, Plaintiff respectfully requests leave to amend the Complaint to reflect damages of $3 billion and additional injunctive relief as stated herein.

Should Defendants continue surveillance during litigation, Plaintiff reserves the right to seek additional punitive damages of $1 million per day.

Given continuing discoveries of foreign involvement, Plaintiff reserves right to seek additional amendments as investigation continues.

Cyber attacks were against:

https://github.com/Caia-Tech/for-world-builders

https://github.com/Caia-Tech/the-burden

https://github.com/Caia-Tech/caiatech.com

theburden.org

caiatech.com

Respectfully submitted,

Marvin Tutt, Pro Se owner@caiatech.com CERTIFICATE OF SERVICE I hereby certify that on June 29, 2025, I served this Motion on all parties through the Court's electronic filing system.

Marvin Tutt EXHIBITS Exhibit A: Maryland Attorney General's Email Response Refusing Investigation Exhibit B: Cloudflare Forensic Reports Documenting Foreign Intelligence Activity

Note: this filing is to correct a previous one. Amended key details and added certificate of service.