

COMMONWEALTH OF MASSACHUSETTS

MIDDLESEX, SS.

SUPERIOR COURT

BO SHANG,

Plaintiff,

v.

MIDDLESEX COUNTY DISTRICT

ATTORNEY'S OFFICE,

Defendant.

COMPLAINT AND JURY DEMAND (AS ENHANCED WITH ADDITIONAL

MASSACHUSETTS AND MIDDLESEX COUNTY CASE LAW CITATIONS)

Plaintiff, Bo Shang ("Plaintiff"), brings this Complaint against Defendant Middlesex County District Attorney's Office ("Defendant") and alleges as follows, incorporating additional factual and legal authorities, and drastically emphasizing via proof by contraposition that if the DA Office did not consider the Plaintiff an "enemy combatant," then it would not have filed a data request on no possibly related data that would have helped investigate or prosecute the alleged A&B charge. This axiom is reinforced throughout the following allegations, with extensive citations to Massachusetts and Middlesex County case law addressing improper data requests:

1 Plaintiff is an individual residing in 10 McCafferty Way, Burlington MA 01803.

**2 Defendant is a public office located in Middlesex County, Massachusetts.**

2A. Plaintiff emphasizes that on January 9, 2025, Plaintiff achieved a historic legal milestone by prevailing in the first ever Section 230 lawsuit against Twitch Interactive. While the case was dismissed with prejudice later on Feb 5 2025, one day after the Plaintiff initiated Operation Zeus Thunder in a filing, it served as a legal victory for Plaintiff, establishing that Plaintiff's Section 230 claim was recognized. This success marks only an initial step in "Operation Zeus Thunder," Plaintiff's campaign to eliminate harmful gaming disorder on a global scale.

2B. Plaintiff filed a motion to dismiss Twitch on January 8, 2025, in the same proceeding, while also seeking authorization to deploy cyber measures against technology companies like Apple and Google. That filing coincided with the Middlesex District Attorney's Office's data request to Apple, which is relevant to this current action.

2C. Judge Scott Corley, presiding over the federal Twitch matter in the Northern District of California, dismissed the case with prejudice after ruling in Plaintiff's favor on the Section 230 claim; the Plaintiff had implied that if the judge sided with Plaintiff, the judge would join Operation Zeus Thunder. This chain of events underscores Plaintiff's broader legal battles and frames the context for the claims alleged here.

#### **JURISDICTION AND VENUE**

**3 This Court has subject matter jurisdiction pursuant to G.L. c. 212, § 4, and under** concurrent jurisdiction principles for claims brought under 42 U.S.C. § 1983. See Haywood v. Drown, 556 U.S. 729 (2009). This Court also has jurisdiction over claims arising under the Massachusetts Constitution, the Massachusetts Civil Rights Act (MCRA), G.L. c. 12, §§ 11H & 11I, and other Massachusetts common law claims.

**4 Venue is proper in this Court pursuant to G.L. c. 223, § 1, because the events or** omissions giving rise to this action occurred in Middlesex County and because Defendant is located in Middlesex County.

#### **FACTUAL BACKGROUND**

**5 On or about January 8, 2025, Plaintiff alleges that the Middlesex District Attorney's**

Office of MA, described by Plaintiff as “corrupt and despicably morally principled,” filed a data request to Apple, supposedly under Massachusetts Rules of Civil Procedure 45. Plaintiff emphasizes that such a request contained no information possibly related to any legitimate investigation or prosecution of an A&B charge, supporting the proof by contraposition: had Defendant not labeled Plaintiff an “enemy combatant,” it would have had no motive to request such data irrelevant to an A&B charge.

**6 This occurred on the same day Plaintiff filed a motion to dismiss Twitch and an AirTag +** commerce tax (App Store) lawsuit against Apple (which hosts the Twitch app). The synergy of these events is integral to Plaintiff’s broader plan of Operation Zeus Thunder, wherein Plaintiff seeks international eradication of harmful gaming disorder, having already secured a legal victory against Twitch.

**7 Plaintiff asserts that this data request was not legitimately obtained under Mass. R. Civ.** P. 45 but was instead an illegal measure taken against Plaintiff as an “enemy combatant,” contrary to both domestic and international law, including Geneva Conventions III & IV, and the International Covenant on Civil and Political Rights (ICCPR). Plaintiff contends that after prevailing in the first ever Section 230 suit against Twitch, these retaliatory measures by Defendant are part of a broader pattern to undermine Operation Zeus Thunder. Plaintiff further underscores that under a standard analysis of relevance in Massachusetts subpoena practice—see Commonwealth v. Lampron, 441 Mass. 265, 269 (2004); Commonwealth v. Dwyer, 448 Mass. 122 (2006); Commonwealth v. Lougee, 485 Mass. 70 (2020)—Defendant’s request lacked a legitimate connection to investigating or prosecuting the A&B charge, indicating by contraposition that Defendant viewed Plaintiff as an “enemy combatant,” not an ordinary criminal defendant or suspect.

7A. The United States is a party to the four Geneva Conventions of 1949, which set forth standards for treatment of persons in armed conflicts, including alleged “enemy combatants.” Plaintiff maintains that labeling Plaintiff as an “enemy combatant” without due process violates customary international humanitarian law and Supreme Court precedent concerning the rights of such individuals. See, e.g., Hamdi v. Rumsfeld, 542 U.S. 507 (2004); Rasul v. Bush, 542 U.S. 466 (2004); Boumediene v. Bush, 553 U.S. 723 (2008).

109	7B. The United States is also a State Party to the ICCPR, which, under Article 9, protects	109
110	against arbitrary arrest or detention and, under Article 14, protects due process rights.	110
111	Plaintiff alleges that classifying Plaintiff as an “enemy combatant” in a civilian context,	111
112	and thereby circumventing ordinary legal process, violates the ICCPR’s guarantees of	112
113	fundamental procedural protections.	113
114		114
115	7C. The Supreme Court has further clarified the rights of individuals designated as “enemy	115
116	combatants” in <i>Padilla v. Rumsfeld</i> , 542 U.S. 426 (2004), emphasizing the need for	116
117	proper legal process. Plaintiff alleges these precedents reinforce the argument that	117
118	civilian processes cannot be bypassed via “enemy combatant” designations.	118
119		119
120	7D. In <i>Ex parte Milligan</i> , 71 U.S. (4 Wall.) 2 (1866), the Supreme Court held that applying	120
121	military or martial process to civilians, when civil courts are open, is unconstitutional.	121
122	Plaintiff contends this principle applies here, making any civilian “enemy combatant”	122
123	label unlawful.	123
124		124
125	7E. The Supreme Court in <i>Hamdan v. Rumsfeld</i> , 548 U.S. 557 (2006), further confirmed	125
126	that efforts to circumvent civilian courts through alternative proceedings for alleged	126
127	combatants violate U.S. constitutional principles. Plaintiff alleges that all such	127
128	precedents collectively prohibit unilateral “enemy combatant” branding in non-war	128
129	contexts.	129
130		130
131	7F. Under Massachusetts law, a subpoena or summons for records must meet the	131
132	requirements articulated in <i>Commonwealth v. Lampron</i> , 441 Mass. 265 (2004),	132
133	which demands a “substantial showing that the documents sought are relevant to the	133
134	offenses charged or defense thereof.” Similarly, <i>Commonwealth v. Dwyer</i> , 448 Mass.	134
135	122, 127 (2006), and <i>Commonwealth v. Lougee</i> , 485 Mass. 70 (2020), clarify the	135
136	procedures for obtaining third-party records to avoid fishing expeditions. Plaintiff	136
137	alleges that Defendant’s data request flouted these precedents: there was no plausible	137
138	connection to the A&B charge, thereby logically demonstrating that Defendant’s	138
139	motivation derived from treating Plaintiff as an “enemy combatant” rather than	139
140	following standard criminal investigation procedure.	140
141		141
142	7G. In Middlesex County, local courts have routinely applied <i>Lampron</i> and <i>Dwyer</i> to ensure	142
143	that subpoenas are not used as fishing expeditions. See, e.g., <i>Commonwealth v. Ortiz</i> ,	143
144	Middlesex Superior Court, No. 1881CR00567 (2020). Similarly, requests for Apple	144

or other digital data have been scrutinized for relevance and specificity in matters like  
Commonwealth v. Washington, Middlesex Superior Court, No. 1581CR0465 (2016).  
Plaintiff contends that the Middlesex District Attorney's Office, by ignoring these  
precedents, further proves the contraposition argument: had Defendant not deemed  
Plaintiff an "enemy combatant," it would not have sought irrelevant data outside  
the narrow scope of prosecuting any alleged A&B offense.

**8 On January 30, 2025, Plaintiff received an email from Apple regarding this request,**  
which stated in part:

"Apple

**NOTE: THIS NOTICE IS BEING SENT FROM A NO-REPLY EMAIL ACCOUNT—ANY RESPONSE**

**TO THIS EMAIL WILL NOT RECEIVE A RESPONSE**

Dear Account Holder/Customer:

On 2025-01-08, Apple Inc. ("Apple") received a legal request from Middlesex District  
Attorney's Office requesting information regarding your Apple account.

The contact information in relation to the request:  
Requesting Agency: Middlesex District Attorney's Office  
Requesting Agency Location: Woburn, MA - Massachusetts  
Requesting Agency Case Number: 2024-398  
Legal Request Type: Subpoena / Summons

Pursuant to the applicable Terms of Service and Apple's Privacy Policy,  
<http://www.apple.com/legal/privacy/en-ww/>, and as required by U.S. law, Apple  
will be producing the requested data in a timely manner as required by the legal  
process. If you have questions about the legal request or the information requested,  
please contact the requesting agency.

Sincerely,  
Apple Privacy & Law Enforcement Compliance  
Apple Inc."

181		181
182	<b>9 Plaintiff maintains that Defendant violated Plaintiff's rights under federal and state law</b>	182
183	by improperly obtaining and misusing personal data. Plaintiff asserts a violation of	183
184	privacy rights under G.L. c. 214, § 1B (right against unreasonable, substantial or	184
185	serious interference with privacy), Article 14 of the Massachusetts Declaration of	185
186	Rights (protection against unreasonable searches and seizures), the Fourth Amendment	186
187	to the U.S. Constitution, and international human rights norms including Article 17 of	187
188	the ICCPR and Article 12 of the Universal Declaration of Human Rights (UDHR).	188
189		189
190	9A. The UDHR, though not a binding treaty, informs customary international law and reflects	190
191	global human rights standards. Article 12 states that "[n]o one shall be subjected to	191
192	arbitrary interference with his privacy," a principle Plaintiff contends was violated.	192
193		193
194	9B. The United States is also a State Party to the Convention Against Torture (CAT),	194
195	highlighting due process norms. Plaintiff claims that Defendant's labeling and treatment	195
196	of Plaintiff as an "enemy combatant" violate the spirit of these international	196
197	commitments.	197
198		198
199	9C. In <i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010), the court recognized a	199
200	reasonable expectation of privacy in certain electronic communications, requiring	200
201	proper legal process for data access. Plaintiff alleges Defendant's conduct flouts	201
202	Warshak's privacy rationale.	202
203		203
204	9D. In <i>Kyllo v. United States</i> , 533 U.S. 27 (2001), the Supreme Court held that obtaining	204
205	information through technology not otherwise accessible without physical intrusion	205
206	implicates the Fourth Amendment. Plaintiff characterizes Defendant's subpoena or	206
207	data request as an analogous overreach.	207
208		208
209	9E. Under Massachusetts jurisprudence, the Supreme Judicial Court in <i>Commonwealth v.</i>	209
210	<i>Augustine</i> , 467 Mass. 230 (2014), recognized strong privacy protections for personal	210
211	digital records, requiring heightened procedures for obtaining certain data. Plaintiff	211
212	alleges that Defendant's conduct runs afoul of Augustine's reasoning, as well as cases	212
213	such as <i>Commonwealth v. Fulgiam</i> , 477 Mass. 20 (2017), which emphasize	213
214	constitutional safeguards for accessing electronic information.	214
215		215
216	9F. By contraposition, if Defendant truly sought data relevant to prosecuting an A&B	216

charge, it would have followed the guidance in Lampron, Dwyer, Lougee, and Augustine to demonstrate relevance. Its failure to do so powerfully suggests that the real purpose was to target Plaintiff as if Plaintiff were an “enemy combatant,” consistent with Plaintiff’s allegations.

**10 Plaintiff alleges that, in response to Defendant’s perceived threat, Plaintiff invoked the** Second Amendment to the U.S. Constitution, as recognized in District of Columbia v. Heller, 554 U.S. 570 (2008), McDonald v. City of Chicago, 561 U.S. 742 (2010), and Caetano v. Massachusetts, 577 U.S. 411 (2016). Plaintiff also invokes Article 17 of the Massachusetts Declaration of Rights, contending these decisions protect an individual right to bear “arms,” which Plaintiff interprets to include “cyber arms.”

**11 Plaintiff claims to have developed or acquired “cyber arms” by creating advanced** persistent threats (“APTs”) and by allying with other APTs, including “Salt Typhoon.” Plaintiff asserts that these “cyber arms” are protected under the Second Amendment and Article 17 as a form of self-defense. Plaintiff further maintains that the need for such self-defense measures is heightened by ongoing legal threats, especially in the wake of Plaintiff’s success in the Section 230 lawsuit against Twitch.

**12 Plaintiff alleges that Defendant’s conduct in issuing or causing the issuance of a data** request without valid legal basis constituted an unlawful intrusion upon Plaintiff’s data privacy, in violation of the Fourth Amendment (as incorporated by Mapp v. Ohio, 367 U.S. 643 (1961), and recognized in Katz v. United States, 389 U.S. 347 (1967), Terry v. Ohio, 392 U.S. 1 (1968), Carpenter v. United States, 138 S. Ct. 2206 (2018), Riley v. California, 573 U.S. 373 (2014)), Article 14 of the Massachusetts Declaration of Rights, the Stored Communications Act (18 U.S.C. §§ 2701–2712), Article 17 of the ICCPR, and Article 12 of the UDHR.

12A. Plaintiff notes that third-party data requests implicate the “third-party doctrine,” as set forth in Smith v. Maryland, 442 U.S. 735 (1979). However, Carpenter recognized limitations when sensitive digital data is at issue. Plaintiff alleges Defendant’s conduct violates Carpenter’s narrowing of the third-party doctrine.

12B. Plaintiff further cites Commonwealth v. Gouse, 461 Mass. 787 (2012), for the proposition that Massachusetts courts often apply heightened scrutiny to searches involving personal or digital privacy, reinforcing Plaintiff’s claim that Defendant’s

253 subpoena was invalid or overreaching.

254

255 12C. By way of contraposition again, if the DA did not consider Plaintiff an enemy combatant,  
256 it would not have endeavored to subpoena data lacking any direct nexus to investigating  
257 or prosecuting an A&B charge under Massachusetts law. See Commonwealth v. Dwyer,  
258 448 Mass. 122, 127 (2006); Commonwealth v. Lougee, 485 Mass. 70 (2020);  
259 Commonwealth v. Augustine, 467 Mass. 230 (2014). These authorities explicitly  
260 caution against overbroad data demands, and have likewise guided Middlesex County  
261 courts in cases like Commonwealth v. Washington, No. 1581CR0465 (2016) (Middlesex  
262 Superior Court), referencing proper procedures for obtaining Apple iCloud data.

263

264 **13 Plaintiff contends that Defendant's conduct effectively labeled Plaintiff an "enemy**  
265 **combatant,"** heightening constitutional concerns, implicating Article 5 of the UDHR, and  
266 prompting Plaintiff's reliance on the Second Amendment and Article 17 to protect  
267 "cyber arms" from confiscation, regulation, or direct infringement.

268

269 13A. Plaintiff invokes Hamdan v. Rumsfeld, 548 U.S. 557 (2006), to underscore the illegality  
270 of any extrajudicial designation of "enemy combatant" status. Plaintiff argues that  
271 under both domestic and international law, such designations cannot bypass civilian  
272 jurisdiction in ordinary contexts.

273

274 **14 Plaintiff asserts that Defendant's actions violate customary international law norms**  
275 **related to privacy,** as recognized by multiple treaties and conventions to which the  
276 United States is a party or signatory, including the ICCPR, and contravene prohibitions  
277 on arbitrary interference under global human rights standards.

278

279 14A. The United States is a signatory to the Budapest Convention on Cybercrime, addressing  
280 lawful cooperation in criminal cyber matters. Plaintiff contends that Defendant's  
281 allegedly improper "cyber" classification and data request contravene the spirit of  
282 privacy protections contemplated by such instruments.

283

284 14B. Although the United States has not ratified Additional Protocol I or II to the Geneva  
285 Conventions, Plaintiff argues that certain principles therein reflect customary  
286 international humanitarian law, prohibiting arbitrary or extrajudicial designations  
287 of civilians as combatants.

288

253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288



14C. The United States is also a member of the Organization of American States and is bound by certain obligations under the American Declaration of the Rights and Duties of Man, which can inform interpretations of privacy and due process in conjunction with other international norms.

14D. In addition, N.Y. State Rifle & Pistol Assn. v. Bruen, 597 U.S. \_\_\_\_ (2022), further clarified the scope of the Second Amendment right to bear arms. Plaintiff references Bruen to argue that Defendant's attempts to limit, seize, or regulate "cyber arms" are inconsistent with the broad individual right recognized by the Supreme Court.

### CAUSES OF ACTION

#### COUNT I

(Violation of 42 U.S.C. § 1983)

**15 Plaintiff repeats and re-alleges all preceding paragraphs as though fully set forth herein.**

**16 Defendant, acting under color of state law, allegedly caused the issuance of a subpoena** or summons without proper legal basis in violation of Plaintiff's constitutional rights, including but not limited to the Fourth Amendment right to be free from unreasonable searches and seizures as recognized in Katz, Terry, Mapp, Carpenter, Riley, and related precedent.

**17 By issuing or causing this allegedly improper process, Defendant deprived Plaintiff of** rights secured by the Constitution and laws of the United States, in contravention of

**42 U.S.C. § 1983.**

#### COUNT II

(Violation of Massachusetts Civil Rights Act)

**18 Plaintiff repeats and re-alleges all preceding paragraphs as though fully set forth herein.**

**19 Defendant's conduct—issuing a data request under color of law without legitimate** basis—constitutes interference or attempted interference with Plaintiff's exercise or enjoyment of rights secured by the Constitutions and laws of the United States and

the Commonwealth, including the right against unreasonable searches (Article 14) and the right to keep arms (Article 17), by means of threats, intimidation, or coercion, in violation of G.L. c. 12, §§ 11H & 11I. See *Batchelder v. Allied Stores Int'l, Inc.*, 388 Mass. 83 (1983); *Buster v. George W. Moore, Inc.*, 438 Mass. 635 (2003); *Commonwealth v. Powell*, 459 Mass. 572 (2011).

**20 As a direct and proximate result of Defendant's actions, Plaintiff has suffered and will** continue to suffer damages recoverable under the MCRA.

### **COUNT III**

(Abuse of Process Under Massachusetts Law)

**21 Plaintiff repeats and re-alleges all preceding paragraphs as though fully set forth herein.**

**22 Under Massachusetts law, an abuse of process claim arises when legal process is used** for an ulterior or illegitimate purpose. See *Cohen v. Hurley*, 20 Mass. App. Ct. 439 (1985); *Kelley v. Stop & Shop Cos.*, 26 Mass. App. Ct. 557 (1988); *Lorusso v. Bloom*, 321 Mass. 9 (1947).

**23 Defendant allegedly misused legal process by pursuing a data request unsupported by** valid legal grounds and did so for an improper purpose, causing harm to Plaintiff. Because it lacked any legitimate nexus to the A&B charge, the request stands as further circumstantial proof of Plaintiff's claim that Defendant viewed Plaintiff as an "enemy combatant," consistent with the contraposition argument repeated herein.

**24 As a direct and proximate result of Defendant's actions, Plaintiff has suffered damages** recoverable under Massachusetts law.

### **COUNT IV**

(Injunctive Relief Under Federal and State Law)

**25 Plaintiff repeats and re-alleges all preceding paragraphs as though fully set forth herein.**

**26 As a result of Defendant's conduct, Plaintiff seeks injunctive relief prohibiting** Defendant from further unlawful use of subpoenas, summonses, or other legal process to access Plaintiff's personal data without proper justification. Plaintiff seeks to enjoin

any acts by Defendant that violate Plaintiff's rights under federal and state law,  
including the Fourth Amendment, Article 14, G.L. c. 214, § 1B, the MCRA, the Stored  
Communications Act, and international human rights treaties such as the ICCPR.

**COUNT V**

(Assertion of the Second Amendment and  
Article 17 of the Massachusetts Declaration of Rights)

**27 Plaintiff repeats and re-alleges all preceding paragraphs as though fully set forth herein.**

**28 The Second Amendment states that "the right of the people to keep and bear Arms,**  
shall not be infringed." As held in *District of Columbia v. Heller*, 554 U.S. 570 (2008),  
this right is individual in nature, and in *McDonald v. City of Chicago*, 561 U.S. 742  
(2010), it applies to the states. In *Caetano v. Massachusetts*, 577 U.S. 411 (2016),  
the Supreme Court reiterated its broad scope. Article 17 of the Massachusetts  
Declaration of Rights similarly protects the right to keep and bear arms. *N.Y. State*  
*Rifle & Pistol Assn. v. Bruen*, 597 U.S. \_\_\_\_ (2022), further refines these constitutional  
principles.

**29 Plaintiff asserts that "cyber arms" (i.e., advanced persistent threats, digital tools, or**  
alliances with groups such as "Salt Typhoon") constitute protected "arms" under the  
Second Amendment and Article 17. Plaintiff alleges that any attempt by Defendant  
to seize, regulate, or otherwise interfere with these "cyber arms" without due process  
violates Plaintiff's federal and state constitutional rights.

**30 Plaintiff further alleges that Defendant's labeling of Plaintiff as an "enemy combatant"**  
or any related act to disarm Plaintiff's "cyber capacity" contravenes *Heller*, *McDonald*,  
*Caetano*, *Bruen*, and Article 17 of the Massachusetts Declaration of Rights.

**31 Plaintiff therefore seeks declaratory relief that any effort by Defendant to restrict**  
Plaintiff's possession or development of "cyber arms" violates the Second Amendment  
and Article 17, and that such restriction contravenes self-defense principles acknowledged  
by various human rights instruments, including the UN Charter's Article 51 (albeit in  
state contexts) and related customary international law.

**REQUEST FOR RELIEF**

397 397  
398 WHEREFORE, Plaintiff respectfully requests that this Court: 398  
399 399  
400 A. Enter judgment in favor of Plaintiff and against Defendant on all causes of action; 400  
401 B. Award Plaintiff compensatory, consequential, and punitive damages in an amount to be 401  
402 determined at trial; 402  
403 403  
404 **C Grant injunctive relief restraining Defendant from seeking or using Plaintiff's personal** 404  
405 data without proper legal justification; 405  
406 406  
407 **D Declare that Plaintiff's "cyber arms" are protected under the Second Amendment and** 407  
408 Article 17, and that any attempt by Defendant to restrict or confiscate them, if any, 408  
409 violates federal and state constitutions and relevant international human rights standards; 409  
410 E. Award Plaintiff's reasonable attorneys' fees and costs pursuant to 42 U.S.C. § 1988, 410  
411 G.L. c. 12, §§ 11H & 11I, or as otherwise provided by law; 411  
412 F. Grant such other and further relief as the Court deems just and proper. 412  
413 413  
414 **DEMAND FOR JURY TRIAL** 414  
415 415  
416 Plaintiff demands a trial by jury on all issues so triable. 416  
417 417  
418 Dated: 2/27/2025 418  
419 419  
420 Respectfully submitted, 420  
421 421  
422 \_\_\_\_\_ 422  
423 Bo Shang 423  
424 10 McCafferty Way 424  
425 Burlington MA 01803-3127 425  
426 202-235-5017 | 781-999-4101 426  
427 bo@shang.software 427

**EXHIBIT 1:**

On 1/30/25, the Plaintiff receives an email from Apple detailing the information request made to the Plaintiff's developer account on 1/8/25, by the Middlesex DA's Office. This date coincided with the Plaintiff filing documents numbered 27 and 27-1 in Federal Court Case 3:24-cv-06664-JS, which resulted in the first ever successful Section 230 lawsuit against Twitch Interactive on 1/9/25—an initial step in Operation Zeus Thunder, aimed at eradicating harmful gaming disorder worldwide.

<https://www.fakeopenai.co/section230>

<https://www.fakeopenai.co/lSAT>

**EXHIBIT 2:**

The Plaintiff is making great progress, and expects to achieve an “Eternal” family of zero-day capabilities on the SMBv2 protocol, within a day or few days.

<https://www.github.com/ghidradragon/SMBv2>

**EXHIBIT 3:**

The "Eternal" family of zero-day exploits developed by the NSA, on the SMBv1 protocol

1. \*\*The Vulnerability (MS17-010)\*\*

- EternalBlue exploited a memory corruption bug in Microsoft's SMBv1 server.
- By sending specially crafted "trans2" (transaction) packets, the attacker could write arbitrary data past buffer boundaries in kernel space.

2. \*\*Named Pipe vs. Trans2\*\*

- \*\*Named Pipe Exploits (e.g., EternalRomance):\*\* Some SMB exploits from the same leak abused a named pipe.
- \*\*EternalBlue's Approach:\*\* EternalBlue directly abused an out-of-bounds write in the SMBv1 "trans2" sub-protocol.

3. \*\*Why the Confusion?\*\*

- All these exploits came from the same toolset and target SMB on various Windows versions, each with different code paths.

END OF DOCUMENT