

COMMONWEALTH OF MASSACHUSETTS

MIDDLESEX, SS.

SUPERIOR COURT

BO SHANG,

Plaintiff,

v.

MIDDLESEX COUNTY DISTRICT

ATTORNEY'S OFFICE,

Defendant.

COMPLAINT AND JURY DEMAND (AS ENHANCED)

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:

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

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

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.

**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).

**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).**

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).

7B. The United States is also a State Party to the ICCPR, which, under Article 9, protects against arbitrary arrest or detention and, under Article 14, protects due process rights. Plaintiff alleges that classifying Plaintiff as an "enemy combatant" in a civilian context, and thereby circumventing ordinary legal process, violates the ICCPR's guarantees of

73 fundamental procedural protections.

74

75 7C. The Supreme Court has further clarified the rights of individuals designated as “enemy  
76 combatants” in *Padilla v. Rumsfeld*, 542 U.S. 426 (2004), emphasizing the need for  
77 proper legal process. Plaintiff alleges these precedents reinforce the argument that  
78 civilian processes cannot be bypassed via “enemy combatant” designations.

79

80 7D. In *Ex parte Milligan*, 71 U.S. (4 Wall.) 2 (1866), the Supreme Court held that applying  
81 military or martial process to civilians, when civil courts are open, is unconstitutional.  
82 Plaintiff contends this principle applies here, making any civilian “enemy combatant”  
83 label unlawful.

84

85 7E. The Supreme Court in *Hamdan v. Rumsfeld*, 548 U.S. 557 (2006), further confirmed  
86 that efforts to circumvent civilian courts through alternative proceedings for alleged  
87 combatants violate U.S. constitutional principles. Plaintiff alleges that all such  
88 precedents collectively prohibit unilateral “enemy combatant” branding in non-war  
89 contexts.

90

91 **8 On January 30, 2025, Plaintiff received an email from Apple regarding this request,**  
92 which stated in part:

93

94 “Apple

95

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

97

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

99

100 Dear Account Holder/Customer:

101

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

104

105 The contact information in relation to the request:

106 Requesting Agency: Middlesex District Attorney's Office

107 Requesting Agency Location: Woburn, MA - Massachusetts

108 Requesting Agency Case Number: 2024-398

73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108

109 Legal Request Type: Subpoena / Summons 109

110 110

111 Pursuant to the applicable Terms of Service and Apple's Privacy Policy,  
112 <http://www.apple.com/legal/privacy/en-ww/>, and as required by U.S. law, Apple  
113 will be producing the requested data in a timely manner as required by the legal  
114 process. If you have questions about the legal request or the information requested,  
115 please contact the requesting agency. 115

116 116

117 Sincerely,  
118 Apple Privacy & Law Enforcement Compliance  
119 Apple Inc." 119

120 120

121 **9 Plaintiff maintains that Defendant violated Plaintiff's rights under federal and state law** 121  
122 by improperly obtaining and misusing personal data. Plaintiff asserts a violation of  
123 privacy rights under G.L. c. 214, § 1B (right against unreasonable, substantial or  
124 serious interference with privacy), Article 14 of the Massachusetts Declaration of  
125 Rights (protection against unreasonable searches and seizures), the Fourth Amendment  
126 to the U.S. Constitution, and international human rights norms including Article 17 of  
127 the ICCPR and Article 12 of the Universal Declaration of Human Rights (UDHR). 127

128 128

129 9A. The UDHR, though not a binding treaty, informs customary international law and reflects  
130 global human rights standards. Article 12 states that "[n]o one shall be subjected to  
131 arbitrary interference with his privacy," a principle Plaintiff contends was violated. 131

132 132

133 9B. The United States is also a State Party to the Convention Against Torture (CAT),  
134 highlighting due process norms. Plaintiff claims that Defendant's labeling and treatment  
135 of Plaintiff as an "enemy combatant" violate the spirit of these international  
136 commitments. 136

137 137

138 9C. In *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), the court recognized a  
139 reasonable expectation of privacy in certain electronic communications, requiring  
140 proper legal process for data access. Plaintiff alleges Defendant's conduct flouts  
141 Warshak's privacy rationale. 141

142 142

143 9D. In *Kyllo v. United States*, 533 U.S. 27 (2001), the Supreme Court held that obtaining  
144 information through technology not otherwise accessible without physical intrusion 144

implicates the Fourth Amendment. Plaintiff characterizes Defendant's subpoena or data request as an analogous overreach.

9E. Under Massachusetts jurisprudence, the Supreme Judicial Court in *Commonwealth v. Augustine*, 467 Mass. 230 (2014), recognized strong privacy protections for personal digital records, requiring heightened procedures for obtaining certain data. Plaintiff alleges that Defendant's conduct runs afoul of *Augustine's* reasoning.

**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.

**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 that 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

181 involving personal or digital privacy, reinforcing Plaintiff's claim that Defendant's  
182 subpoena was invalid or overreaching.

183  
184 **13 Plaintiff contends that Defendant's conduct effectively labeled Plaintiff an "enemy**  
185 **combatant,"** heightening constitutional concerns, implicating Article 5 of the UDHR, and  
186 prompting Plaintiff's reliance on the Second Amendment and Article 17 to protect  
187 "cyber arms" from confiscation, regulation, or direct infringement.

188  
189 13A. Plaintiff invokes *Hamdan v. Rumsfeld*, 548 U.S. 557 (2006), to underscore the illegality  
190 of any extrajudicial designation of "enemy combatant" status. Plaintiff argues that  
191 under both domestic and international law, such designations cannot bypass civilian  
192 jurisdiction in ordinary contexts.

193  
194 **14 Plaintiff asserts that Defendant's actions violate customary international law norms**  
195 **related to privacy,** as recognized by multiple treaties and conventions to which the  
196 United States is a party or signatory, including the ICCPR, and contravene prohibitions  
197 on arbitrary interference under global human rights standards.

198  
199 14A. The United States is a signatory to the Budapest Convention on Cybercrime, addressing  
200 lawful cooperation in criminal cyber matters. Plaintiff contends that Defendant's  
201 allegedly improper "cyber" classification and data request contravene the spirit of  
202 privacy protections contemplated by such instruments.

203  
204 14B. Although the United States has not ratified Additional Protocol I or II to the Geneva  
205 Conventions, Plaintiff argues that certain principles therein reflect customary  
206 international humanitarian law, prohibiting arbitrary or extrajudicial designations  
207 of civilians as combatants.

208  
209 14C. The United States is also a member of the Organization of American States and is bound  
210 by certain obligations under the American Declaration of the Rights and Duties of Man,  
211 which can inform interpretations of privacy and due process in conjunction with other  
212 international norms.

213  
214 14D. In addition, *N.Y. State Rifle & Pistol Assn. v. Bruen*, 597 U.S. \_\_\_\_ (2022), further  
215 clarified the scope of the Second Amendment right to bear arms. Plaintiff references  
216 *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.

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

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

**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.

**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**

WHEREFORE, Plaintiff respectfully requests that this Court:

- A. Enter judgment in favor of Plaintiff and against Defendant on all causes of action;
- B. Award Plaintiff compensatory, consequential, and punitive damages in an amount to be determined at trial;

**C Grant injunctive relief restraining Defendant from seeking or using Plaintiff’s personal data without proper legal justification;**

**D Declare that Plaintiff’s “cyber arms” are protected under the Second Amendment and**

Article 17, and that any attempt by Defendant to restrict or confiscate them, if any,  
violates federal and state constitutions and relevant international human rights standards;  
E. Award Plaintiff's reasonable attorneys' fees and costs pursuant to 42 U.S.C. § 1988,  
G.L. c. 12, §§ 11H & 11I, or as otherwise provided by law;  
F. Grant such other and further relief as the Court deems just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury on all issues so triable.

Dated: 2/27/2025

Respectfully submitted,

\_\_\_\_\_  
Bo Shang  
10 McCafferty Way  
Burlington MA 01803-3127  
202-235-5017  
typhoonenigma@icloud.com

361  
362  
363  
364  
365  
366  
367 **EXHIBIT 1: On 1/30/25, the Plaintiff receives an email from Apple detailing the information request made to**  
368 **the Plaintiff's developer account on 1/8/25, by the Middlesex DA's Office. This date coincided with the**  
369 **Plaintiff filing 27 and 27-1 in Federal Court Case 3:24-cv-06664-JS, the first time ever anyone has won a**  
370 **Section 230 claim vs Twitch interactive.**  
371  
372 <https://www.fakeopenai.co/section230>  
373  
374 <https://www.fakeopenai.co/lsat>  
375  
376  
377  
378  
379  
380  
381  
382  
383 **EXHIBIT 2: The Plaintiff is making great progress, and expects to achieve an "Eternal" family of zero-day**  
384 **capabilities on the SMBv2 protocol, within a day or few days.**  
385  
386 <https://www.github.com/ghidradragon/SMBv2>  
387  
388  
389  
390 **EXHIBIT 3: The "Eternal" family of zero-day exploits developed by the NSA, on the SMBv1 protocol**  
391  
392 **## A Bit More Detail**  
393  
394 **1 \*\*The Vulnerability (MS17-010)\*\***  
395 - EternalBlue exploited a memory corruption bug in Microsoft's SMBv1 server (in functions like  
396 `Srv!SrvOs2FeaListToNt` or `Srv!SrvTransaction2Dispatch`).

397 - By sending specially crafted "trans2" (transaction) packets, the attacker could write arbitrary data past  
398 buffer boundaries in kernel space (in particular, in the `SRV` driver).  
399

## 400 2 \*\*Named Pipe vs. Trans2\*\* 400

401 - \*\*Named Pipe Exploits (e.g., EternalRomance):\*\* Some SMB exploits from the same leak abused a  
402 named pipe—often `\\pipe\SRVSVC`—to hold open a file/pipe handle in the SMB server and then  
403 manipulate buffer offsets for code execution. 403

404 - \*\*EternalBlue's Approach:\*\* EternalBlue directly abused an out-of-bounds write in the SMBv1 "trans2"  
405 sub-protocol. While SMBv1 does support named pipes, EternalBlue's trigger was not contingent on  
406 obtaining a pipe handle. 406

## 407 3 \*\*Why the Confusion?\*\* 407

408  
409 - All these exploits came from the same toolset (Equation Group's FuzzBunch) and target SMB on various  
410 Windows versions. 410

411 - EternalBlue, EternalRomance, EternalChampion, and EternalSynergy each had different code paths and  
412 slightly different vulnerabilities, even though they were all SMB-related. 412

413 413

414 --- 414

415 415

416 ### Summary 416

417 417

418 - \*\*EternalBlue\*\* = Exploits a buffer overflow in SMBv1's "trans2" commands. 418

419 - \*\*Does it use a pipe?\*\* No—unlike some sibling exploits (e.g., EternalRomance), it does \*\*not\*\* hinge on  
420 a named pipe handle. 420

**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 27 and 27-1 in Federal Court Case 3:24-cv-06664-JS, the first time ever anyone has won a Section 230 claim vs Twitch interactive.

<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

#### ## A Bit More Detail

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

- EternalBlue exploited a memory corruption bug in Microsoft’s SMBv1 server (in functions like `Srv!SrvOs2FeaListToNt` or `Srv!SrvTransaction2Dispatch`).
- By sending specially crafted “trans2” (transaction) packets, the attacker could write arbitrary data past buffer boundaries in kernel space (in particular, in the `SRV` driver).

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

- \*\*Named Pipe Exploits (e.g., EternalRomance):\*\* Some SMB exploits from the same leak abused a named pipe—often `\\pipe\\SRVSVC`—to hold open a file/pipe handle in the SMB server and then manipulate buffer offsets for code execution.
- \*\*EternalBlue’s Approach:\*\* EternalBlue directly abused an out-of-bounds write in the SMBv1 “trans2” sub-protocol. While SMBv1 does support named pipes, EternalBlue’s trigger was not contingent on obtaining a pipe handle.

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

- All these exploits came from the same toolset (Equation Group’s FuzzBunch) and target SMB on various Windows versions.
- EternalBlue, EternalRomance, EternalChampion, and EternalSynergy each had different code paths and slightly different vulnerabilities, even though they were all SMB-related.

---

#### ### Summary

- \*\*EternalBlue\*\* = Exploits a buffer overflow in SMBv1’s “trans2” commands.
- \*\*Does it use a pipe?\*\* No—unlike some sibling exploits (e.g., EternalRomance), it does **not** hinge on a named pipe handle.