MATTHEW R. WALSH
19197 GOLDEN VALLEY RD #333
SANTA CLARITA, CA 91387
(661) 644-0012

Plaintiff In Pro Per,

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

MATTHEW R. WALSH Plaintiff In Pro Per, vs. ROKOKO ELECTRONICS (AND DOES 1 THROUGH 50, INCLUSIVE) Defendant	Case No.: 2:25-CV-05340-ODW-RAO Before: Hon. Otis D. Wright II Courtroom 5D **MOTION FOR PROTECTIVE ORDER AGAINST DEFENDANT ROKOKO ELECTRONICS FOR CONTINUED ACCUSATIONS OF FELONY MISCONDUCT OR IN THE ALTERNATIVE, TO STRIKE.**

BACKGROUND

The Plaintiff lawfully procured all data; Rokoko simply doesn't "like" what it proves. Because they cannot challenge the evidence's substance, they have pivoted to attacking the Plaintiff's character. Rokoko's own counsel admitted to a total lack of technical comprehension, stating the evidence *"might as well be Russian to me."*

When pressed in discovery to identify anyone capable of interpreting this data, Rokoko hid behind boilerplate objections, claiming that their ability to understand the facts *"is not relevant to any claims or defenses."* It is both improper and dangerous for Defendants to baselessly accuse the Plaintiff of "felony activity" while simultaneously admitting they lack the basic literacy required to understand the technology or evidence involved. This Court must address these scandalous and uninformed smears.

INTRODUCTION

Defendants' attempt to characterize standard network auditing as "wiretapping" is technically and legally absurd. Under their logic, viewing data on a monitor is lawful, but observing those same packets on a network card attached to the same computer is a felony—an interpretation that would criminalize every IT professional and router in California. Furthermore, alleging a "Man-in-the-Middle" attack in a two-party exchange is a physical impossibility; there cannot be a man in the middle when only two parties exist; it's literally in the name.

These scandalous claims of "felonious hacking" are a transparent attempt to mask Defendants' lack of technical competency and entirely avoid the substance fo the evidence against. Rokoko has labeled hundreds of technologically definitive terms "vague and ambiguous" while simultaneously admitting the evidence *"might as well be Russian"* to them. This is akin to a colorblind witness testifying to the

color of a traffic light, or a layman accusing a surgeon of "assault with a deadly weapon" post-surgery because they lack the basic understanding of surgery. This issue goes directly to competence. Rokoko cannot credibly claim evidence is "fabricated" when they admit they simply cannot read the language it is written in. This is not a legal defense; it is a scandalous character assassination fueled by willful ignorance and must be stricken under FRCP 12(f).

Their goal is clear: to disqualify all adverse evidence from now through trial and more urgently, to avoid an unsavory ruling on Plaintiff's dispositive motion where they brought (a) no contrary evidence (b) no expert and; (c) have created no genuine dispute.

Plaintiff respectfully requests the Court:

(a) ENTER a protective order against Rokoko:

a. to prevent them from continuing to make baseless, harmful and claims regarding the legality of Plaintiff's evidence

b. to prevent them from continuing to perpetuate the "hacker" narrative

c. to prevent them from continuing to accuse the Plaintiff of felony behavior, as this is the third time.

(b) STRIKE the record of the above references, particularly in their Dkt #173 filings (more specifically but not limited to #173-3, #173-4)

ARGUMENT

I. I. The Technological Absurdity ("The Internet Argument")

The technology "Stack" which nearly every interconnected device relies upon is not a crime scene: If merely observing already-existing packets between a local client and a remote server is "eavesdropping," then every network diagnostic tool and antivirus program—from McAffee to Windows Event Viewer to Wireshark—is a felony device. To accept Defendant's conjecture and argument is to criminalize the basic architecture of the internet (Network Cards, Sockets, CPUs, Routers and Modems). To accept their logic and apply it to law would produce only one end-result: **turning off the internet completely.**

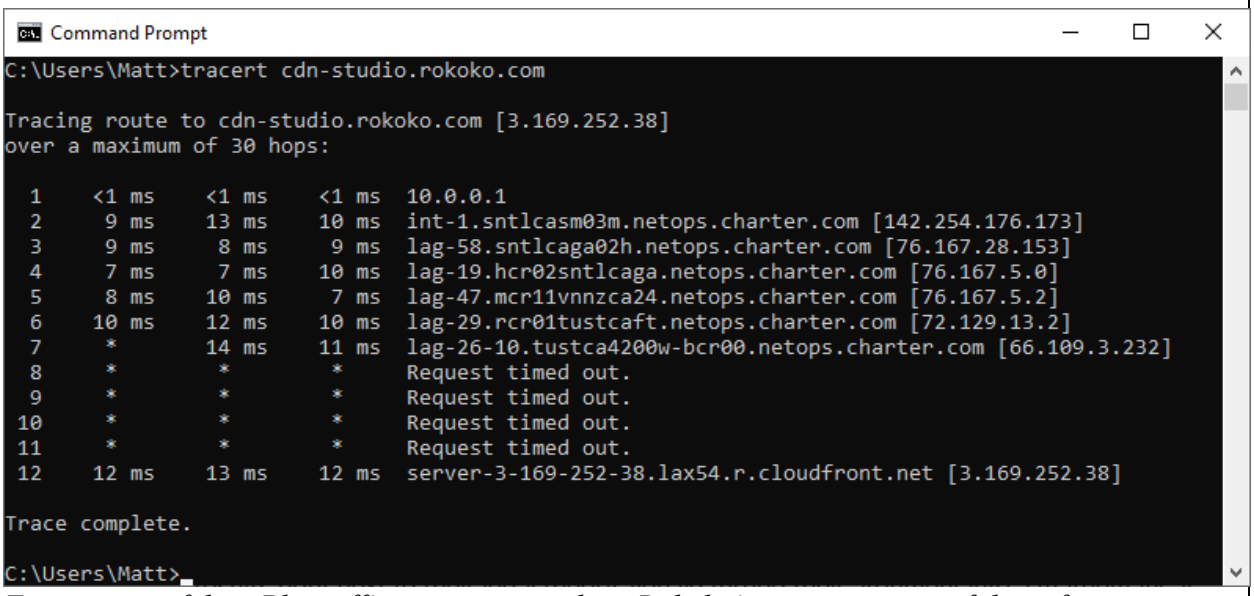
Illustration 1.0:

The OSI Model

The Open Systems Interconnection (OSI) model is a conceptual, seven-layer framework developed by the ISO to standardize network communications. It breaks down complex data transmission into smaller, manageable layers—from physical cabling (Layer 1) to user applications (Layer 7)—ensuring different systems can communicate, troubleshooting is simplified, and technology interoperability is maintained

			Rokoko's Logic	Reality
7	Application Layer	Human-computer interaction layer, where applications can access the network services	Plaintiff using Rokoko Studio and it's communications and data is legal.	Rokoko software needs layers 1 - 6 to make layer 7 even possible.
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs	Plainitff being aware of the data's content and structure he was just using is a felony.	The data is assembled on Plaintiff's machine, then encrypted using a two-party SSL certificate. Plaintiff holds one half of the key, Rokoko holds the other.
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions	Plaintiff's antivirus and firewalls which passively handle connections are felony wiretapping tools.	The data moves passively through multiple systems and layers which can see the data before it even is transmitted to or from Rokoko. This is required design.
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP	The TCP/IP and WebSockets protocols which facilitate the entire communication are felony tools.	There exists an entire network stack which requires the passive digestion of this data as network packets contain To, From, Data Payload, etc.
3	Network Layer	Decides which physical path the data will take	Each "hop" the data must travel to is a new wiretap by a third-party and are independent felonies.	For one data packet to go from Plaintiff's PC to Rokoko's servers, it passes through 12 devices. Each one of those devices are privy to that data.
2	Data Link Layer	Defines the format of data on the network	The determination of the data format by a machine means the data was analyzed by felony software layers.	The data link layer expressly deals with pareparing the data for transmission across the physical layer.
1	Physical Layer	Transmits raw bit stream over the physical medium	The network card, wires, modem, local router, C.O., WAN routers are all felony wiretap devices.	For 12 hops, 55 components would be felony devices; at 60 packets per second, 4,200 felonies would be commited per second.

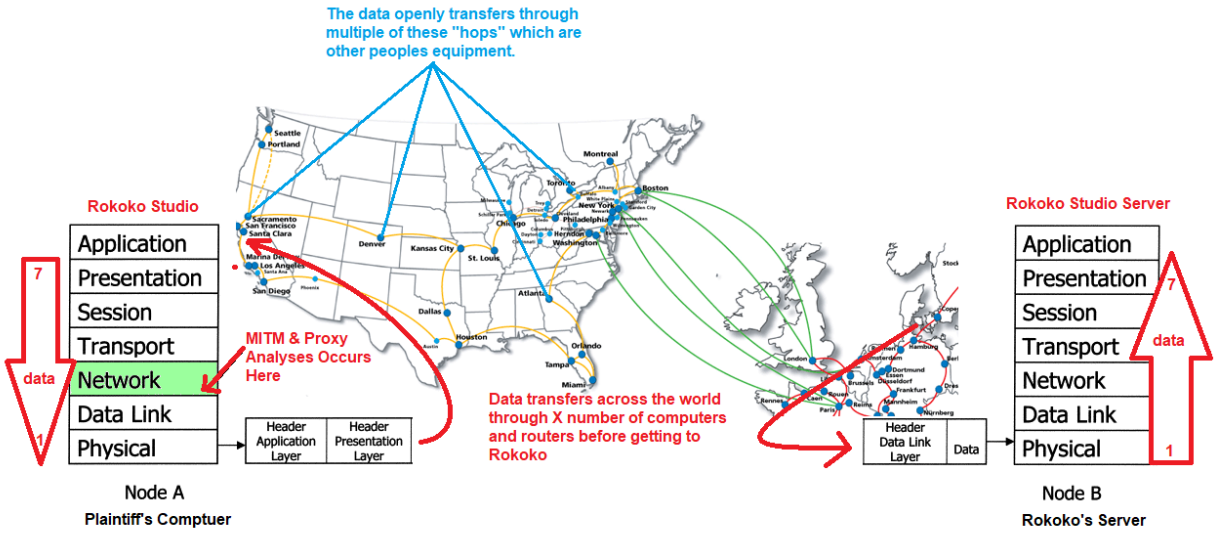
Illustration 1.1:



Every piece of data Plainitff's computer sends to Rokoko's servers in use of the software goes through twelve computers/routers first.

Observation vs. Interception: Plaintiff did not "break in" to a third-party conversation. Plaintiff sat on his own "digital porch" (his own hardware/OS) and observed the "digital creek" (data packets) flowing on his own property to which he has the metaphorical equivalent of “water rights” over. He simply looked at that stream of data, flowing on his physical property, through it, and out into a public lake (“the internet”) where no one; neither Rokoko or the Plaintiff has any control or expectation over it’s accessibility or privacy.

Illustration 2:



The internet is a “web” computers are interconnected and act together in concert both passively and actively to achieve the transmission of data. The data passes through no less than 288 layers from Walsh to Rokoko (accounting for the redundancy of the 7-layer OSI model). Plaintiff monitored the data at position 5 of 288. Each of these 288 points sees the same data Plaintiff observed.

II. The Legal Failures of Invoking PC § 632

First, There was no *"Confidential Communication"*: PC § 632 applies to human-to-human speech where there is a *"reasonable expectation of privacy."* Background API calls and automated JSON handshakes between software and a server are not *"confidential communications."* They are technical transactions.

Second, the Defendant conveniently ignored the remainder of PC 632:

> *"(c) For the purposes of this section, "confidential communication" means any communication ... **confined to the parties** thereto... excludes a communication made in a public gathering .. which the parties to the communication may reasonably expect that the communication may be overheard or recorded."*

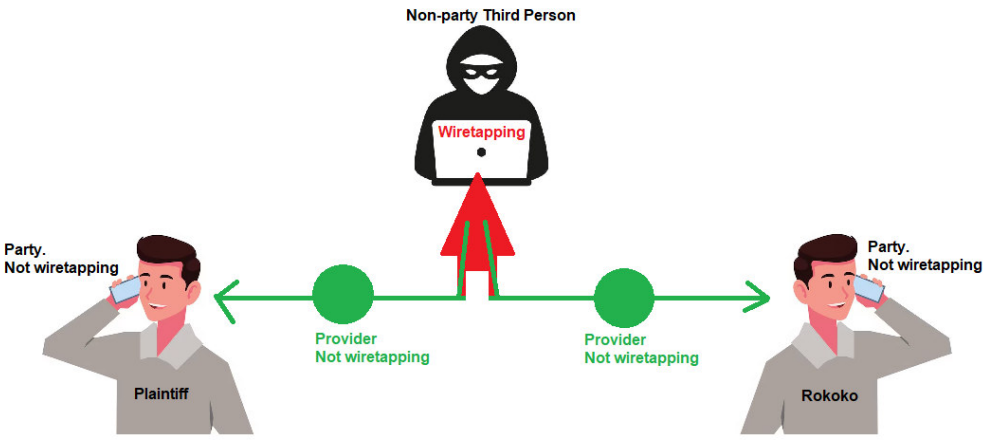
For the reasons already established, technologically it would be impossible for the communications to be confined to the parties as the inherent ways that the internet makes communications possible in the first place *(Flanagan v. Flanagan - 27 Cal.4th 766 S085594).* Moreso, Plaintiff and Rokoko *are the parties of the communication*, there was no disallowed, unauthorized third party listener. No action of the Plaintiff changed that fact, nor the transmission or data in any capacity.

Third, the internet (not the providers or their equipment themselves) is a peer-to-peer operating public property; and upholds the constitutional protections of freedom of speech and communication rights. In Reno v. ACLU 521 U.S. 844 (1997), the Court ruled that internet communication deserves the same high level of First Amendment protection as a speaker on a street corner soapbox.

III. The "Party to the Communication" Rule:

Rokoko's conjecture fails at a number of turns. **First,** because the communications are already in written/text format, recording in any medium falls under one-party consent (18 U.S.C. § 2511(2)(d)). The Electronic Communications Privacy Act (ECPA) provides that it is not unlawful for a person to intercept an electronic communication if that person is a party to the communication.

Illustration 3:



The only way a "man in the middle attack" could occur, is if there is a third person – in the middle of two authorized parties' communication.

Second, California is a "two-party" consent state for recording of "**conversations"**. Just as a party to a text message conversation does not have to notify the other party it was recorded in sending that message; Digital communications too are already 'in writing'. One cannot be liable for possessing evidence of a written communication to which they are a party unless it is "confidential." Even if the Defendant found a way to argue it is speech, since Plaintiff was the one "speaking" (sending the data), he had full authority to screen shot a written record his own "speech"; just as he would a text-message sent to or from him.

IV. The Communications Are Admissible:

The Defendant argues that even if Plaintiff has a right to access the communications, the content is inadmissible as it is hearsay, however, this argument fails as well:

First, FRE 801(d)(2)): Statements made in a text or written format are generally not considered hearsay because they *are "admissions by a party-opponent"* and can be used directly against them.

Second, There is no expectation of privacy in sent messages. Federal and state courts consistently hold that once a text is sent, the sender loses control over it. In Commonwealth v. Diego, 166 A.3d 1259 (Pa. Super. 2017) and State v.

Patino, 93 A.3d 40 (R.I. 2014), courts ruled that individuals have no reasonable expectation of privacy in sent text messages because they cannot prevent the recipient from sharing or saving them.

Third, evidence obtained is admissible if it is to be used as **proof** in an action for violation of the section. Precisely this is what has occurred. Rokoko themselves are accused "through espionage or other means" of actually intercepting in true "man in the middle" fashion and harvesting Plaintiff's private data without authorization, sending harmful code to Plaintiff's computer and misappropriation of the same. If anyone meets the criteria of CA PC 632, it is the Defendant Rokoko. Therefore, obtaining proof of that violation of CA PC 632 is in itself qualifying as an exception to inadmissibility thereof:

> *"(d)* ***Except as proof in an action*** *... evidence obtained as a result of eavesdropping upon or recording a confidential communication ... is not admissible"*

//

V. Witnessing A Crime Generally Does Not Create A Second Crime

Rokoko is attempting to claim a "privacy right" to take Plaintiff's data in violation of the CFAA, CA PC without Plaintiff being allowed to see them do it. The Penal Code was designed to protect individuals from government/corporate overreach, not to protect corporations from being caught in the act of data

harvesting, espionage, intellectual property infringement and so forth. The Defendants have been accused of multiple actions since the initial Complaint which has the ability to rise to felony-level conduct.

To that instance, the law absconds away from Defendants characterization that Plaintiff is simply being a petulant law breaker and instead shifts towards the conversation towards characterizations parallel under the whistleblower doctrine:

(First) 18 U.S.C. § 2511(2)(g)(iv) states that it is not unlawful for any person to intercept a wire or electronic communication which is being used to facilitate a crime. **(Second)** a party who happens upon evidence of a crime and preserves it is generally protected under the "Public Interest" exception, **(Third)** while usually applied to Attorney-Client privilege, the Crime-Fraud Exception is a broader doctrine that states no privilege or privacy protection exists for communications made in the commission or concealment of a crime. **(Fourth)** United States v. Leon 468 U.S. 897 (1984) provides that Plaintiff's reasonably belief that his actions were necessary to document a crime, Plaintiff would lack the *mens rea* for a second crime to be established. Fifth, *United States v. Steiger, 318 F.3d 1039 (11th Cir. 2003)*(finding that even if a private party's search was unauthorized, it did not violate the Fourth Amendment because the person was not a government agent, and the evidence was admissible) and; **(Sixth)** CA PC § 632(d) states that while *"confidential communications"* are usually inadmissible if

recorded, they are admissible in a proceeding *"for the purpose of proving the commission of a felony."*

//

VI. The Van Buren Shield (The "Supreme Court" Argument)

Authorized Access: Under Van Buren v. United States, the security "gates" were up. In Walsh v. Rokoko, there were no “gates”. Plaintiff had authorized access to the suit(s) he own[ed], has an authorized user account, was expressly authorized to use the software and was a party to the communications.

No Circumvention: Plaintiff did not bypass any security "gates" to access the data; he simply used a passive "magnifying glass” (the MITM proxy software stack) to visualize the communications he was already privy to. Van Buren makes it clear that using authorized access for a purpose the company dislikes is not a crime.

//

VII. Rokoko Must Engage An Expert Moving Forward

Pursuant to FRCP 12(f), the Court may strike "redundant, immaterial, impertinent, or scandalous matter." Rokoko continues to weaponize scandalous and baseless claims—labeling evidence "fabricated and fanciful"—while repeatedly refusing to engage competent experts to interpret the data. Instead of addressing the merits, Defendants have launched a defamatory campaign outside the Court,

disparaging Plaintiff to an audience of 10 million by calling him "crazy" and accusing him of fraud. Because Rokoko lacks expert testimony to refute the evidence, they have resorted to attacking the material as "inadmissible", “illegal”, “felonious” and attacking Plaintiff personally. These unfounded assertions serve only to prejudice the record and should be stricken and a protective order entered against future statements. Courts continuously find that litigants cannot answer technical questions outside of the knowledge of a layperson and *must be addressed by expert testimony.* Many of these cases resulted in disposition at summary judgment due to this very fact. The same should be found here as well in the interest of judicial economy. *(see also Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993), Chastain v. Poynter Law Group, No. 2:18-cv-01254 (C.D. Cal. Sept. 30, 2020), Smash Technology, LLC v. Smash Solutions, LLC, 335 F.R.D. 438 (D. Utah 2020), M2M Solutions LLC v. Motorola Solutions, Inc., 167 F. Supp. 3d 673 (D. Del. 2016), Sargon Enterprises, Inc. v. University of Southern California, 55 Cal. 4th 747 (2012), Federal Rule of Evidence 702: Explicitly requires that scientific, technical, or specialized knowledge be provided by a qualified expert)*

CONCLUSION

Plaintiff didn't "hack" anything. He observed his own data. Defense Counsel doesn't understand the technology they accuse Plaintiff of misusing while remaining disinterested in having constructive conversations regarding it. Rokoko has refused discovery, while simultaneously calling the Plaintiff a criminal for looking at the very data they said he already had in his possession — which, if anything, exposes their conduct. Rokoko must be stopped from continuing to make these baseless claims, if they wish to continue, they should be made to do so through expert opinion, not attorney argument lacking factual basis and threshold understanding of basic technology function.

PRAYER FOR RELIEF

Plaintiff respectfully asks the Court:

1. STRIKE Defendants evidentiary objections in (Dkt #173-3) which conflict with the principles in this motion.

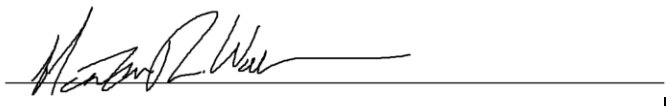
2. ENTER a protective order so that Defendant may no longer assert claims of computer hacking, nor felony statutes in relation thereof.

3. ORDER that the Defendant must retain an expert witness if they wish to continue challenging the Plaintiff's expertise or credibility in relation to the technological concepts placed before the Court.

4. ORDER the Defendant to pay Plaintiff expert fees, costs or sanctions due to the harmful accusations and the need to prepare this motion.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed March 8, 2026



Matthew R. Walsh
Plaintiff In Pro Per