

**VIRGINIA:**

**IN THE APPELLATE COURT  
OF VIRGINIA**

COMMONWEALTH OF VIRGINIA	)	
	)	CAV RECORD NO. 1950-19-4
v.	)	
	)	FAIRFAX COUNTY CIRCUIT COURT
NORMAN ACHIN	)	CASE NO. FE-2018-1497
Defendant	)	
_____	)	

**AMICUS CURIAE BRIEF FROM BONNIE BURKHARDT  
IN SUPPORT OF DEFENDANT NORMAN ACHIN**

Bonnie Burkhardt, *pro se* litigant  
President, Senior Engineer  
**BLUE RIDGE SOFTWARE CONSULTING**  
8402 Gambrell Lane  
Springfield, VA 22153  
(703)505-2793  
Bonnie.burkhardt@blueridge-sw.com

1. Table of Contents

1. Table of Contents ..... ii

2. Table of Authorities ..... iii

3. Interest of Amicus Curiae ..... 1

4. Summary of Argument ..... 2

    4.1 Communication Privacy Issues through the Ages ..... 2

    4.2 Issues Before the Court ..... 4

5. Argument ..... 9

    5.1 All Party Consent to Intercept and Record Private Communications ..... 9

    5.2 One Party Consent to Intercept and Record Private Communications ..... 10

        A. Can Officers Impersonate Real People? ..... 13

        B. Identity Theft ..... 17

        C. Can Officers Control Imaginary People? ..... 18

        D. Nuances of Statutory Verbiage ..... 20

        E. Interpreting Va. Code § 18.2-374.3 as Subordinate to § 19.2-61, *et seq.* ..... 21

        F. Using a Phone as an Interception Device ..... 21

        G. Reverse Targeting of U.S. Citizens ..... 22

        H. Electronic Warfare against U.S. Citizens ..... 23

    5.3 Searching Computers and Electronic Devices ..... 25

        A. Searching a Confiscated Device ..... 25

        B. Hash Codes Identifying Content ..... 26

        C. Hash Codes are Protected by the Stored Communication Law ..... 27

        D. Hash Codes used to Populate the Database and Send Notifications ..... 31

        E. Remotely Searching Computers ..... 33

        F. User Errors Affected by Hash Codes and Third-Party Malicious Intent ..... 35

        G. Geo-location via Photographs ..... 37

    5.4 Authority Expressly Granted to Intercept ..... 37

    5.5 Question for the Court: Does Va. Code § 18.2-374.3 Criminalize Teen Dating? ... 38

6. Conclusion ..... 40

## 2. Table of Authorities

### Cases

<i>Ashcroft v. Free Speech Coalition</i> , 122 S. Ct. 1389 (2002).....	14
<i>Cogdill v. Commonwealth</i> , 219 Va. 272. (1978) .....	15
<i>Commonwealth v. Einuis</i> (Fairfax County, 2014) .....	15
<i>Commonwealth v. Hawthorne</i> (Stafford County, 2016).....	12, 19, 25
<i>Commonwealth v. Lopez</i> (Amelia County, 2016).....	passim
<i>Commonwealth v. Witalec</i> (Stafford County, 2016).....	39
<i>Crislip v. Commonwealth</i> , 37 Va. App. 66, 71-72, 554 S.E.2d 96, 98-99 (2001).....	21
<i>Dietz v. Commonwealth</i> , 294 Va. 123, 804 S.E.2d 309, 2017 Va. LEXIS 117 (2017) .....	16
<i>Grafmuller v. Commonwealth</i> , 290 Va. 525 (2015).....	15
<i>Hix v. Commonwealth</i> , 042717 (Va. 2005).....	19
<i>Katz v. United States</i> , 389 U.S. 347 (1967) .....	3, 9
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001).....	33
<i>Last v. Virginia State Board of Medicine</i> , 14 Va. App. 906 (1992) .....	21
<i>Lawrence v. Texas</i> , 539 U.S. 558 (2003).....	40
<i>Oregon v. Combest</i> , 350 P. 3d 222 - 2015 .....	34
<i>Rose v. Locke</i> , 423 U.S. 48 (1975).....	11
<i>Sorrells v. United States</i> , 287 U.S. 435 (1932).....	12
<i>State v. Hinton</i> , 87663–1 (Wa. 2014) .....	13
<i>State v. Roden</i> , 41037–1, 41047–8–II (Wa. App., 2012).....	13
<i>U.S. v. Campagnuolo</i> , 556 F.2d 1209 (5th Cir. 1977), .....	12, 15
<i>U.S. v. George</i> , No. 19-4125 (4th Cir. 2020).....	18
<i>U.S. v. Hoeffener</i> , No. 19-1192 (8th Cir. 2020).....	8, 31, 34
<i>U.S. v. Jones</i> , 565 U.S. 400 (2012).....	32, 37
<i>U.S. v. Katzin</i> , No. 12-2548 (3d Cir. 2013) .....	37
<i>U.S. v. Perrine</i> , 518 F.3d 1196 (10th Cir. 2008).....	30
<i>U.S. v. Polequaptewa</i> , (8:16-cr-00036 District court, D.D. Calif. 2018). .....	37
<i>U.S. v. Thayer</i> , 154 F. 508, (June 17, 1907) .....	11

## Statutes

18 U.S.C. § 1028.....	14, 15, 17
18 U.S.C. § 1028A.....	18
18 U.S.C. § 2510.....	6, 22
18 U.S.C. § 2511.....	passim
18 U.S.C. § 2515.....	7, 42
18 U.S.C. § 2701.....	passim
47 U.S.C. § 225.....	3
50 U.S.C. § 1801.....	4, 6, 15
50 U.S.C. § 1821.....	3, 33
50 U.S.C. § 1881a.....	23
Md. Code § 10-401.....	10, 22
Md. Code § 10-402.....	10, 16, 17
Va. Code § 18.2-186.3.....	14, 15, 17
Va. Code § 18.2-370.....	16
Va. Code § 18.2-374.1.....	36
Va. Code § 18.2-374.3.....	passim
Va. Code § 19.2-61.....	6, 21, 22, 28
Va. Code § 19.2-62.....	passim
Va. Code § 19.2-65.....	7, 16, 42
Va. Code § 19.2-70.....	32, 33

## Other Authorities

Americans with Disabilities Act (1990) .....	3
BitTorrent Usage (January 2020).....	28
Computer Decency Act of 1996 .....	39
Electronic Communications and Privacy Act (ECPA) of 1986.....	1
Executive Order 12333, <i>United States Intelligence Activities</i> (1981) .....	3, 4, 15
Foreign Intelligence Surveillance Act of 1978, Amendments Act of 2008 (FISA) .....	1, 23
Grindr’s User Agreement, July 1, 2018.....	22
Joint Publication 3-13.1 <i>Electronic Warfare</i> (2012): .....	24
Microsoft Windows 10 BitTorrent (December 18, 2018) .....	29
Office of DNI, <i>Civil Liberties and Privacy Guidance for Intelligence Community Professionals: Properly Obtaining and Using Publicly Available Information</i> , July 2011 .....	31, 35
OVSC1203: FISA Amendments Act Section 702 Class Transcript.....	4, 15, 16, 23
<i>Report on Investigations Involving the Internet and Computer Networks</i> , Department of Justice (DOJ), Office of Justice Programs, (January, 2007).....	3, 9, 29, 32
Shareaza User’s Manual (online) (Feb. 2, 2014) .....	passim
United States Signal Intelligence Directive (USSID SP0018) <i>Legal Compliance and U.S. Persons Minimization Procedures</i> .....	10

### **3. Interest of Amicus Curiae**

I, Bonnie Burkhardt, filed a motion with the Court and was granted leave to file an *amicus curiae* petition for appeal in this case.

I affirm and attest that I have an interest in this matter since I am a network protocol engineer with over 35 years of experience in telecommunications. I worked for General Telephone and Electronics (GTE) Government Systems for a decade beginning in 1984. It provided secure communications, electronic surveillance systems, and electronic warfare systems to the Department of Defense (DoD). I then switched to digital signal analysis (digital signal forensics), developing software tools, techniques, and training on analyzing signals intercepted by the DoD. I am a certified system administrator for a government computer network. *See Appendix 2.*

As a 35-year engineer and signal analyst for the DoD, I receive twenty refresher classes a year on the Electronic Communications and Privacy Act (ECPA) of 1986, Foreign Intelligence Surveillance Act (FISA), and other privacy laws. I am legally obligated to report anyone I believe is violating Federal law. Since this case involves privacy issues for phone calls, text messages, and private messages exchanged over the internet via a dating app, my experience and training at the Federal level is relevant.

My reputation and standing in my neighborhood of 30 years has been permanently marred due to improper application of these laws and police tactics used. These tactics were used against Christopher Hawthorne, a member of my church, who pled guilty to violating Va. Code § 18.2-374.3. After serving his sentence, Mr. Hawthorne registered as sex offender but was not allowed to live with his wife and children until he satisfied certain Court-imposed criteria. My husband and I offered to let him stay in our home, and he accepted. Instantly, our home became tagged as

a “registered sex offender home.” Our neighbors received alerts on their phones. Emails circulated to dozens of people that we were hosting a sex offender. My next-door neighbor excoriated me. Neighbors across the street still refuse to talk to us.

#### **4. Summary of Argument**

This brief discusses Fourth Amendment protections in the Electronic Age. I found no caselaw showing testimony of a network protocol engineer familiar with ECPA.

##### **4.1 Communication Privacy Issues through the Ages**

Communication privacy and authentication has been an issue since ancient times. The story of Jacob impersonating his brother Esau in Genesis 27:34–40 illustrates this problem. Rebekah overhears her husband, Isaac, and their son, Esau, discussing a blessing. She convinces the younger Jacob to impersonate his brother and call Isaac, which Jacob does. Jacob successfully tricks his father into bestowing the blessing upon him instead of his brother. Suppose this story happened using today’s technology and Jacob instead records Isaac’s phone call. Is it lawful for Jacob to record the phone call while impersonating Esau because of one-party consent - Jacob is “a person and such person is party to the conversation?” Is the content of this conversation admissible in Court as an authentic conversation between Isaac and Esau? Between Isaac and Jacob? Or is it inadmissible? Does the answer change if Jacob is a Virginia police officer with no “color of law” exception for police?

Letters, phone calls, and text messages represent historical progression of personal communications. Letters were signed for authentication. Envelopes were sealed for privacy. Wax seals impressed with a signet ring authenticate the author. Broken seals indicated privacy violations. With the invention of telephones, one identifies the other speaker by recognizing the

voice speaking. Deaf persons depend on the phone number and TDD/TTY operator to authenticate the caller. It would be unethical for an operator to hear a *man*'s voice, but type onto the TDD/TTY screen suggesting it is a 13-year-old *girl* speaking. Text messages were found to provide TDD/TTY capability. Americans with Disabilities Act (1990) codified 47 U.S.C. § 225.

New forms of communications cause new privacy challenges. One's right to a private conversation is protected even when using a public phone booth. In *Katz v. United States*, 389 U.S. 347 (1967), police attached a listening device to the outside of a public telephone booth. The Supreme Court ruled this a search and seizure of one's private communications. The use of technology to survey the interior of a private space is considered a search protected by the Fourth Amendment. In 1978, Congress codified 50 U.S.C. § 1821, expanding 'physical search' to include "examination of the interior of property by technical means."

Watergate triggered review of existing communication privacy laws. In 1981, President Reagan signed Executive Order 12333, *United States Intelligence Activities* (1981), EO12333, defining "electronic surveillance" as "acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of nonelectric communications, without the consent of a person who is "**visibly present.**" (emphasis added) *Appendix 1 at 15, sec. 3.5(c)*. Though derivative laws, a persona must be capable of satisfying the **visibly present** criteria in order to be a party to an electronic communication. See 18 U.S.C. § 2511(2)(d), Va. Code § 19.2-62(B)(2); *Report on Investigations Involving the Internet and Computer Networks*, Department of Justice (DOJ), Office of Justice Programs, (January, 2007), *Appendix 3 at 25, 75*.

The meaning of "person" does not change mid-sentence. Replaying history: Nixon could record conversations in the Oval Office only if he was visibly present (Nixon Tapes), or if he was



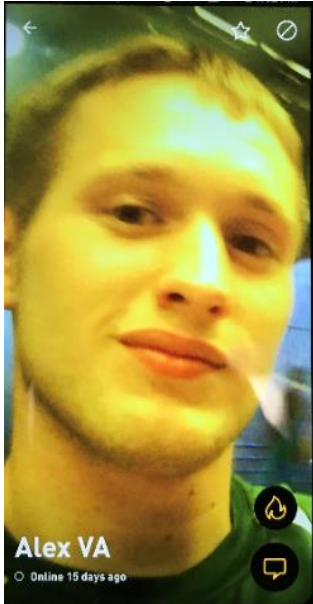
party to the phone call; recording in the Watergate hotel room was disallowed. This expanded to include the intentional acquisition of private radio communications (cell phone signals) if both the sender and all intended recipients are located within the United States. *See* 50 U.S.C. § 1801(f)(3) and OVSC1203: FISA Amendments Act Section 702 Class Transcript, *Appendix 11 at 24*.

Congress codified EO12333 into the Electronic Communications and Privacy Act of 1986 (ECPA). This legislation afforded electronic communications the same privacy protections as phone calls and letters. Title I protects privacy of electronic, wire, and oral communications in transit, including routing path detailing how a message travels from point A to point B and ownership of electronic accounts. Title I is known colloquially as the “wiretap law,” but includes authentication and other methods of obtaining private communications beyond old-style wiretapping. Title II, the Stored Communications Act, governs stored electronic communications and transactional records. If Congress allowed for imaginary people to intercept communications, the Watergate Defense might have claimed an imaginary person was hiding under the Watergate hotel bed, recording.

Virginia has enacted its own more restrictive version of ECPA Title I, expressly omitting a “color of law” exception for state and local law enforcement. *See* Va. Code § 19.2-61 et seq.

#### **4.2 Issues Before the Court**

**First Issue - The Court erred when it denied defendant Norman Achin’s motion to suppress internet chats and recordings of telephone conversation between Achin and Alex / Alex VA.** *See Appendix 18 at 16:21-17:13.*



If this was a picture of Det. Bauer disguised as Alex VA, Bauer would have been projecting the persona of Alex VA and would have been party to the electronic messages exchanged. (R. at 000850). That did not happen. If the person pictured spoke with Achin on the recorded phone calls, then the person pictured would have been party to those conversations. That did not happen. Instead, Det. Gadell spoke on the phone.

The Court erred because the young man pictured, Alex VA, was not party to any electronic or oral communications, though he was the intended recipient of Achin’s communications. No warrant was issued prior to obtaining Achin’s communications. *See Appendix 16 at 15:22-16:1.* Yet the Court determined that fact irrelevant. *See Appendix 16 at 17:9.* The young man pictured was an officer, not a minor, and this crime involves a minor. *See Appendix 16 at 22:5-14.*

CW Attorney Lowe argued that because Bauer was the recipient of Achin’s messages, Bauer was also the intended recipient. *See Appendix 18 at 8:2-9:2.* However, “intended recipient” is clearly defined in Va. Code § 19.2-62(C). Bauer was not an agent of Alex VA, not employed by Alex VA, not acting at Alex VA’s direction. Alex VA was a creature invented by Bauer, deployed as a deception to be the intended recipient of Achin’s messages. Alex VA “is not a person, it cannot give permission to record” any electronic or oral communications. *See Appendix 18 at 16:13-17 and 5:3-9.*

In its motion, Defense explained that interception of communications here is not analogous to the common “football interception” comparison. “In fact, a message can be intercepted at the

exact same time the message is also received.” (R. at 000040-000042). The Court was confused about the meaning of “interception,” though the defense clarified it. *See Appendix 18 at 12:3-23*. The prosecution confused the issue again by implying the “football interception” analogy was the only way interception could occur. *See Appendix 18 at 13:7-14:1*. This confusion led to denial of the suppression motion. *See Appendix 18:16:21-17:13*.

In *U.S. v. Szymuszkiewicz*, — F.3d —, 2010 WL 3503506 (7th Cir. September 9, 2010), Szymuszkiewicz was convicted for being a recipient, though not the intended recipient, of emails sent to his boss. Szymuszkiewicz was a system administrator who secretly setup auto-forwarding on his boss’s account so copies of emails would also be sent to him. In other words, the football pass completed without interception. A duplicate, second football appeared; this second football was carried for an illegal touchdown. Football rules further prohibit the defensive back from wearing the offensive receiver’s jersey to trick the quarterback into throwing the football (i.e. Bauer tricked Achin). Old-fashioned wiretaps are not the only way to intercept communications.

Bauer intercepted cell phone transmission and message content; the person pictured received neither. *See* 50 U.S.C. § 1801(f)(3). “Intercept means any aural or other means of acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.” Va. Code § 19.2-61 and 18 U.S.C. § 2510. Similarly, in two recorded phone calls, Achin thought he was speaking to the young male pictured, but the person pictured was not party to the phone call. Neither was Bauer party to the phone call; he was standing nearby listening as Gadell talked on the phone. *See Appendix 16 at 6:23-7:6 and 8:15-21*. A distinction must be made between ‘participant’ in a conversation and ‘person party to’ a conversation. Although Gadell participated in the call, Achin was the only lawful party to the conversations.

The faithless friend doctrine does not apply here either, since the “friend” in the picture was not party to any conversations and could not authorize the recordings. *See Appendix 18 at 16:21-17:13.*

There was no probable cause for Bauer to be on Grindr investigating a crime. *See Appendix 16 at 16:2-6.* Interception and recording apparently began with the stranger saying, “hello” on an adult-only dating site. That stranger was Mr. Achin. What probable cause exists after uttering “hello” that would justify interception and recording of Achin’s private conversation while in the privacy of his home? Not only is unauthorized interception a felony and a federal crime, but also any “endeavor to intercept.” Va. Code § 19.2-62(A)(1) *and* 18 U.S.C. § 2511(1)(a).

Intercepted content of private text and voice communications was the primary evidence against Achin. Both state and federal law allow a person to intercept their own conversation. There is no provision permitting impersonators or imaginary people to intercept as “*such person is a party to the conversation*” cannot be satisfied. Prosecution incorrectly stated the contrary: “there’s nothing in the wiretap code ... when the person you were speaking to wasn’t the person...” *Appendix 18 at 8:13-16.* If Bauer was impersonating Alex VA in the photo, then Bauer was not “such person” who was party to the conversation. If Alex VA is an imaginary person created and controlled by Bauer and imaginary people don’t really exist, then Alex VA has no legal standing to do anything.

Defendant’s motion to suppress evidence should be granted on the grounds that evidence was not legally obtained. Bauer and Gadell intercepted communications between Achin and a fictitious person, Alex VA, in violation of Va. Code § 19.2-65 and 18 U.S.C. § 2515. These

intercepted communications formed the basis of the evidence against Achin and should be suppressed, charges against Norman Achin dropped.

**Second Issue - search and seizure.** Evidence in snapshots of Achin's phone show Grindr using a live internet connection, e.g. "Online 15 days ago". See phone icons. (R. at 000850, 000872). Police procedures require any phone in evidence to be put in a Faraday-type box to prevent internet connections and corrupting of evidence. Could evidence from Grindr be obtained without this live connection? The search warrant was for Achin's phone, not his remote Grindr account.

While interrogating Achin, Det. Bauer discussed hash codes used to identify changes to content on Achin's devices. *See Appendix 15 at 03 (101)*. Hash codes are used to flag remote internet computers containing suspicious files or illicit photos, for potential police investigation. Although law enforcement can remotely access a computer to search file listings and content, a warrant must be obtained. However, police frequently search private, password protected computers over the internet without a search warrant. They download file listings and content, then manufacture the pretext of "probable cause." They also fail to obtain a pen register warrant before researching the Internet Protocol (IP) address to obtain the owner's name and address. Police download content, then use it *post facto* to justify obtaining a search warrant for the physical address to locate the computer there. They search the house and confiscate the computer. A second warrant obtained to search the confiscated computer confirms the original unwarranted remote search, resulting in arrest and prosecution.

Law Enforcement uses hash codes when creating a database containing content inventory of citizen's private computers. Police use a tool capable of bypassing passwords and gaining entry to a device, contrary to the detective's testimony in *U.S. v. Hoeffener*, No. 19-1192 (8th Cir. 2020).

Police secured no warrant to obtain this data. As the database is periodically updated, any newly identified computers holding “illegal” files trigger alerts. Warrantless geo-location of the IP address triggers an alert to law enforcement for that geographic location. Police then seek the computer at this IP address.

## 5. Argument

Electronic messages have the same privacy protections as phone calls. “... any person who: 1. Intentionally intercepts, endeavors to intercept or procures any other person to intercept or endeavor to intercept, any wire, electronic or oral communication; ... shall be guilty of a Class 6 felony.” (emphasis added). Two concepts stem from Va. Code § 19.2-62:

1. A person who is party to a private conversation is one human with one birth certificate.
2. One must be capable of “pulling off” the persona in face-to-face conversation in order to use the persona for online private chats or in a phone call.

Achin had a reasonable expectation of privacy. *See Appendix 3 at 76.* He was in his private home or car with the door closed when using his cell phone. *See Katz v. United States.* His phone was protected with “electronic locks,” passcode or username / password. *See Riley v. California*, 134 S. Ct. 2473 - 2014. He had a password-protected router in the communication path adding to his assumption of privacy. Achin communicated via private phone calls and electronic messages, which are protected by ECPA. *See Appendix 16 at 9:15-23.*

### 5.1 All Party Consent to Intercept and Record Private Communications

Bauer intercepted communications while in Maryland, outside his Fairfax County, Virginia jurisdiction (*see Appendix 16 at 6:9-13*). Maryland considers interception of oral or electronic communications a felonious offense unless all parties consent. *See Md. Code § 10-402(c)(3)*

(*Appendix 4 at 6*). Achin did not consent. Bauer was not investigating violations of Maryland law. *See* Md. Code § 10-402(a)(1), § 10-402(b) (*Appendix 4*) and 18 U.S.C. § 2511(1)(a). Bauer was not acting under Maryland authority. *See* Md. Code § 10-401(11). VA Commonwealth Attorney did not research Maryland wiretap law in the seven months between the pre-trial and the trial on May 21, 2019. At trial the Commonwealth and Bauer willfully used and disclosed the entire content of the conversation with Achin, including portions intercepted from Maryland. *See* Md. Code § 10-402(a)(2) and § 10-402(a)(3) in *Appendix 4*, 18 U.S.C. § 2511(1)(c), and § 2511(1)(d). *See* United States Signal Intelligence Directive (USSID SP0018) *Legal Compliance and U.S. Persons Minimization Procedures, Appendix 5 at 13 sec. 5.4.*

## **5.2 One Party Consent to Intercept and Record Private Communications**

Bauer and Gadell each claimed to be the “one party” who consented to interception and recording of Achin’s communications. The facts in Achin’s case present two concerns: 1. Bauer and Gadell impersonated the person pictured, violating the “such person is a party to the conversation” clause; 2. They formed an imaginary person by combining characteristics of three different people: Bauer texting, Gadell’s voice on the phone, and a third officer as the person in the picture, i.e. three birth certificates. This combination violates the legal definition of “person” as set forth in “We, the People...” and Article IV of the Constitution. A “person” is not a composite of three humans formed to give the illusion of one human. A “person” has one birth certificate.

Black’s Law Dictionary, 9<sup>th</sup> ed. defines “person” as a human being or the living body of a human being; “impersonate” means the act of impersonating someone; and “persona” means an individual human being. Webster’s dictionary 2018 ed. adds that “persona” is a social façade or

the personality one projects in public. Precise definition is of such importance that, “Even trained lawyers may find it necessary to consult legal dictionaries,” *Rose v. Locke*, 423 U.S. 48 (1975).

ECPA uses the term “person” to define who has rights and can be “a party to the communications.” The General Assembly has expressly adopted in Va. Code § 19.2-62(B)(2) federal statutory language. Both federal and state statutes refer to “a person” singular, “such person” (not “such people”), and “is a party” (not “are parties”). Nowhere does it refer to imaginary persons:

*It shall not be a criminal offense under this chapter for a person to intercept a wire, electronic or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.*

Imaginary people cannot give consent to anything. *See Appendix 18 at 5:3-6.*

U.S. Supreme Court Justice Holmes wrote the majority opinion in *U.S. v. Thayer*, 154 F. 508, (June 17, 1907), clarifying that solicitation crimes via mail only occur “if it takes place in the intended way.” “If the letter has miscarried” (delivered to someone else), “the defendant would not have accomplished a solicitation.” Bauer was not the addressee. “Nothing less than bringing the offer to the actual consciousness of the person addressed would do” (emphasis added) Imaginary people have no consciousness. “An offer is nothing until it is communicated to the party to whom it is made.” The male pictured never read the messages nor saw the pictures, so “the offense was not complete, but, when it had been read.”

It is well-established in law that a person (human being) can intercept and record one’s own conversations or authorize someone else to record them. One cannot install a recording device on one’s home phone to record the conversations of a cheating spouse, for “*one of the parties to the communication has*” NOT “*given prior consent to such interception.*” Va. Code § 19.2-62



(B)(2). Surveillance cameras do not record audio because of these statutes - the person recording is not visibly present. Bauer “put a recording device on it [the phone] to record” Achin talking to Alex VA. *See Appendix 18 at 10:22-11:1*. Achin was tricked into believing he received a call from Alex VA; yet Gadell impersonated Alex VA’s voice. Similarly, in *Commonwealth v. Hawthorne* (Stafford County, 2016), Det. Wells used a recording device to capture live feed video and audio when Wells was not the intended recipient. *See Va. Code § 19.2-62(A)(2), 18 § U.S.C 2511(1)(b)(i) and Appendix 12 at 1*.

By comparison, here are examples of lawful interception:

1. An undercover officer can wear a disguise, meet a drug dealer, and record electronic and oral conversations exchanged. *See Sorrells v. United States*, 287 U.S. 435 (1932). Here, the same officer who is projecting a persona is the same person communicating, whether by phone, online, or in person – one birth certificate.
2. Perhaps a parent notifies police of a suspicious person contacting their child online. The officer obtains parental permission to record the conversations between the child and the suspect. Police supervise and advise the child as the child converses. The child becomes “such person who is a party to the conversation,” and the child becomes “one of the parties to the communications [who] has given consent to such interception.” One child, one birth certificate.
3. If officers are conducting a valid search of premises with a warrant and the phone rings, they may answer the phone and converse - provided they give their true names. *See U.S. v. Campagnuolo*, 556 F.2d 1209 (5th Cir. 1977). No warrant was issued prior to obtaining Achin’s communications, yet the Court ruled this failure to obtain authorization to intercept communications was irrelevant. *See Appendix 16 at 15:22-16:1*. No search was being

executed at the time in Achin's home. The officers did not answer Achin's phone, they initiated a call to Achin.

So, was the young male depicted in the photo party to the conversations? He could not be because he did not participate in any communication. Was Bauer impersonating the young male in the photo? If so, "such person" in the photo was **not** party to the conversation. Or did Bauer manufacture an imaginary person? If so, cobbling together a composite profile consisting of texting by Bauer, the visual image of the young male, and the voice by Gadell does not meet the legal definition of "a person."

#### **A. Can Officers Impersonate Real People?**

Can an officer lawfully impersonate someone else to obtain private electronic, oral, or wire communications from an unwitting second party? Can an officer post a picture of someone else and lawfully pretend to be them? *See* Va. Code § 19.2-62(B)(2) or Va. Code § 18.2-374.3. The faithless friend doctrine does not apply here because one's friend is not betraying him. *See Appendix 18 at 16:21-17:13*. One's "friend" is an impersonation.

If Congress or the General Assembly intended to grant law enforcement authority to impersonate someone else in this way, it would have expressly stated it. In Washington State, a drug dealer was arrested; the detective then impersonated the dealer. The detective sent text messages from the dealer's confiscated phone to arrange meetings with buyers Hinton and Roden. They each met the officer. Both were arrested. Washington Supreme Court overturned the convictions of Hinton and Roden reasoning that text messages are a "private affair" and are protected against warrantless intrusion via impersonation. *See State v. Hinton*, 87663-1 (Wa. 2014) and *State v. Roden*, 87669-0 (Wa. 2014).

When Bauer was asked to send a picture of himself, he did not dress up in a disguise and send a photo of himself as “Alex VA.” Using a photo or being visibly present are two ways of establishing identification. Instead, he transmitted a photo of another adult male, not otherwise involved in this case. *See Appendix 16 at 22:5-14*. The U.S. Supreme Court ruled that statutes can only be applied to images of “real” children. The provision that an image “is, or appears to be, of a minor” was ruled overbroad and may not even indicate exploitation of real children. *See Ashcroft v. Free Speech Coalition*, 122 S. Ct. 1389 (2002). A young officer is not a minor, and this crime involves minors.

A photo is a “means of identification” showing unique physical characteristics of a person, *see* 18 U.S.C. § 1028(a)(7), § 1028(d)(7)(B), and Va. Code § 18.2-186.3(C). Bauer created the character of the 14-year-old “Alex VA” solely for the purpose of intercepting communications and inducing people to commit a crime. He assigned Alex VA’s character traits to the young male pictured, not to himself. The male pictured was not party to any communication. Achin’s replies, intended for the male pictured, were intercepted by Bauer and used to further the conversation. “Alex VA” by himself has no birth certificate.

The young male pictured was not party to the phone calls either. Bauer procured Gadell to be the voice of “Alex VA”. *See Appendix 16 at 6:21-7:6, 14:11-21*. Gadell was procured solely to obtain Achin’s oral communications, “to sound younger.” *Appendix 18 at 11:2-4*. State and federal statutes preclude one from procuring another person to intercept electronic or oral communications. *See* Va. Code § 19.2-62(A)(1) and 18 U.S.C. § 2511(1)(a).

Since Bauer’s phone sent the text messages, it was also used for the phone call so the caller ID would match. A phone number is a “means of identification,” 18 U.S.C. § 1028(a)(7), § 1028(d)(7)(B), and Va. Code § 18.2-186.3(C). The call was then recorded. *See Appendix 16*

7:5-6. Bauer was not party to the conversation. *Ibid* 8:18-21. If Gadell had given his true name (vs. “Alex”) on the phone call, he could have lawfully recorded the conversation. *See U.S. v. Campagnuolo*. If the male pictured had spoken on the phone, he might have authorized his phone call to be recorded. *See Cogdill v. Commonwealth*, 219 Va. 272. (1978). In *Grafmuller v. Commonwealth*, 290 Va. 525 (2015), one female officer presented herself as a 13-year-old girl in emails and phone calls. However, it is unclear if that female officer met the “visibly present” criteria required of EO12333, in order for it not to be considered an impersonation. *See Appendix 1 at 15, sec. 3.5(c)*.

In Achin’s case, Bauer, Gadell, and the male in the photo all project the same persona “Alex VA.” Yet, “persona” means the social façade one person projects in public, not three. Bauer and Gadell impersonated the male pictured. The one and only flesh-and-blood “person” and true party to the conversation was Achin, and he did not authorize any interception or recording. There is **no** “color of law” exception in Va. Code § 19.2-62.

Similarly, in *Commonwealth v. Einuis* (Fairfax County, 2014), Det. Boffi procured another person’s identity in order to obtain communications exchanged with Einuis. Concerned parents turned over their son’s cell phone to Boffi. Einuis had not yet communicated anything unlawful according to his attorney. Boffi obtained parental permission to impersonate, though he had **no legal authority** to do so. *See Appendix 11 at 26*. Boffi sent messages from the son’s phone so the caller ID would match, a “means of identification,” under 18 U.S.C. § 1028(a)(7), § 1028(d)(7)(B), and Va. Code § 18.2-186.3(C). Boffi induced Einuis to reply with messages that violated Va. Code § 18.2-374.3. Replies were sent to the son, but Boffi intercepted the cell phone signal and content. *See* 50 U.S.C. § 1801(f)(3). The son was not party to the conversation. Boffi used the content to continue the conversation until he manufactured sufficient evidence to justify an arrest.

Einuis' arrest warrant clearly states the crime did not involve the youth, but rather Boffi posing as an "undercover operation alleged 14-year-old male." *Appendix 9*. Einuis' legal counsel failed to consider Fourth Amendment protections of Va. Code § 19.2-62 before advising Einuis to accept the plea deal.

Court held that there is no requirement to prove communications involve a third party. *See Dietz v. Commonwealth*, 294 Va. 123, 804 S.E.2d 309, 2017 Va. LEXIS 117 (2017). *Dietz* argued that impersonation is not allowed pursuant to Va. Code § 18.2-370 and § 18.2-374.3. However, *Dietz* failed to argue that § 19.2-62 precludes anyone from impersonation online to intercept communications, even law enforcement, even when parental permission is given. *See Appendix 11* at 26.

Einuis' conversations were disclosed to the press and school system, asking the public to come forward with additional information. *See* Va. Code § 19.2-68(F)(1). Additional charges were subsequently filed against Einuis based on evidence "derived therefrom" via impersonation.

Likewise, Achin's conversations were disclosed to the Court and used as the basis for charges brought against him. *See* Va. Code § 19.2-65. Within 24-hours, the Fairfax Police Department issued a press release about his arrest, disclosing the content of his private conversations out of context. However, using or disclosing the content of communications obtained via an unauthorized intercept is prohibited. *See* Va. Code § 19.2-62(A)(3,4), Md. Code § 10-402(a)(2,3), and 18 U.S.C. § 2511(1)(c,d).

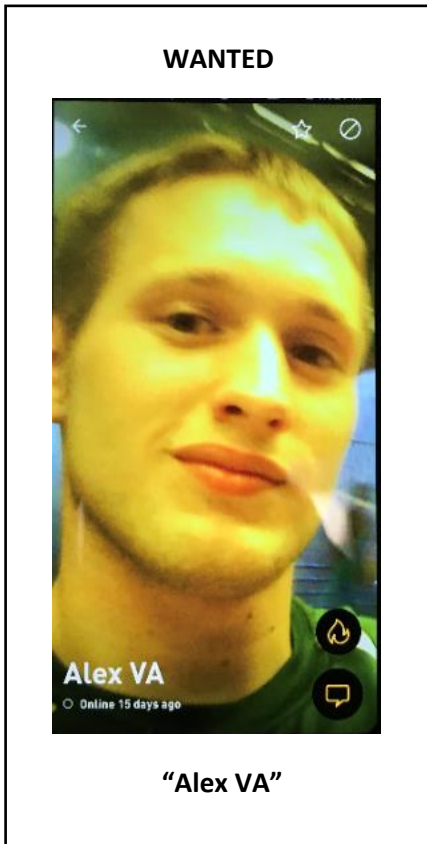
When police unlawfully disclose and broadcast intimate details of someone's private life, it can irreparable damage lives and have far reaching effects. Mr. Achin is plaintiff in civil litigation involving the custody of his special needs child. Attorney Ellen Dague, GAL, and an

unnamed Legal Services employee were present at Achin's pretrial hearing on Oct. 17, 2018. They both "had reason to know the conversations were obtained from interception" since they both heard Attorney Stephen Sheehy argue the communications were intercepted in violation of Virginia's ECPA law. Both also heard Bauer testify he was in Maryland during some of the interceptions. (*see Appendix 16 at 6:9-13*). After pre-trial, one or both of them willfully informed opposing counsel as to the content. In April, Kempczynski used the intercepted content to propound discovery on Achin. Defense did not research Maryland wiretap laws. At trial, Kempczynski further disclosed the contents of private communications to the Alexandria Circuit Court and to those assembled in the gallery. *See* Va. Code § 19.2-62(A)(3,4), Md. Code § 10-402(a)(2,3), and 18 U.S.C. § 2511(1)(c,d).

## **B. Identity Theft**

Identity theft is another way in which law enforcement actions are far from simple investigative techniques, but a serious violation of law. "Whoever ... knowingly ... uses, without lawful authority, a means of identification of another person ... in connection with, any unlawful activity" violates 18 U.S.C. § 1028(a)(7). One's photo reflects a person's unique physical characteristics and is a "means of identification." Bauer's physical attributes do not match the "Alex VA" photo. Bauer procured the "means of identification" of someone else solely to intercept electronic communications with Achin. *See* Va. Code § 18.2-186.3(C) and § 19.2-62(A)(1). Bauer and Gadell had no legal authority to intercept Achin's communications because they were NOT the intended recipient of those communications – the male identified by the photo was the intended recipient. Bauer had no legal authority to use another person's photo as a "means of identification" on Grindr, either.

In *U.S. v. George*, No. 19-4125 (4th Cir. 2020), the court held that the definition of “person” includes those living and deceased, pursuant 18 U.S.C. § 1028A(a)(a). The officer pictured is alive. Bauer’s use of someone else’s photo as his own identification to intercept communications meets the definition of identity theft.



A “WANTED” poster consists of an identifying photo and either one’s actual name, e.g. John Dillinger, or a persona name, e.g. “Billy the Kid.”

Whom would the police be looking for based on this hypothetical “WANTED” poster? (R. at 000850)

The young officer in the photo?

Det. Bauer without a toupee?

Det. Bauer is clearly not the young male pictured.

### **C. Can Officers Control Imaginary People?**

Can an officer then lawfully manipulate an imaginary person online to obtain private electronic, oral, or wire communications exchanged with an unwitting second party under Va. Code § 19.2-62(B)(2) or Va. Code § 18.2-374.3? The Sixth Amendment guarantees a defendant

the right “to be confronted with the witnesses against him,” but how can this happen when the “victim” / true witness is an imaginary person who does not exist?

Imaginary people are like cartoons - a visual image combined with dialogue and an actor’s voice. Cartoons and imaginary people have no rights, have no legal standing as persons, and have no birth certificate. Since a cartoon is not a human with a certificate of live birth, it cannot be a person party to a conversation. *See* Va. Code § 19.2-62(B)(2). The faithless friend doctrine also does not apply here; your friend is not betraying you. Your “friend” is an imaginary person who does not exist and, like cartoons, do not experience friendship or faithfulness. It has no legal standing to intercept or record conversations.

Imaginary people do not live lives. They do not age. Therefore, how can an imaginary people be “under” age when they can never age and grow older? “Age” is defined as the length of time during which a person has lived. *See* Black’s Law Dictionary, 2<sup>nd</sup> ed. The imaginary person “Heather Boon” (persona of Det. Wells) was 13 years old in 2001 (*see Hix v. Commonwealth*, 042717 (Va. 2005)), but only age 14 in 2012 (*see Commonwealth v. Hawthorne*, Appendix 12 at 1).

Similarly, Robo callers can be imaginary people also participating in conversations. A computer manipulates a Robo caller voice using either a computer-generated voice or by playing a person’s recorded voice. Although Robo callers “participate” in conversations, federal ECPA law prohibits Robo callers from recording unless a warning is first given: “This call may be monitored or recorded.” This law applies equally to text messages. *See* Va. Code § 19.2-62(A). Computers have no birth certificates. While they may “participate” in calls, they cannot be a ‘party to conversations.’



Technology exists to manufacture the illusion of a human online – consider computer games. Computers combine visual images, voice, and dialogue to project a life-like person talking and moving in whatever manner is typed into the keyboard. No matter the technology involved, imaginary people are not “human beings capable of having rights.” They cannot legally be a “person” who is party to the conversation. Illusions have no birth certificates.

Google experimented with these concepts and ran afoul of the law. It combined artificial intelligence, a computer-generated voice, and technology that hears and understands human speech. On May 8, 2018, Google instructed its computer to call a hair salon and make an appointment while Google recorded the call. The call participants were Google’s computer and a live receptionist – one machine and one human. Within weeks, Google had to preface all such calls with “this call may be monitored.”

#### **D. Nuances of Statutory Verbiage**

Laws do not protect imaginary people. Va. Code § 18.2-374.3 prescribes the means by which solicitation of an actual minor can occur. The statute offers five subtle but distinct characterizations of its key phrase, “has reason to believe” the child is underage:

*Soliciting ... any child he knows or has reason to believe is at least 15 years of age*  
*Soliciting ... the child he knows or has reason to believe is less than 15 years of age* (2x)  
*Soliciting ... any person he knows or has reason to believe is a child younger than 15 years of age*  
*Soliciting ... any person he knows or has reason to believe is a child younger than 18 years of age*

Note, the gerund “*soliciting*” has the direct objects “*child*” and “*person*,” meaning human beings having rights. It is followed by adjectival clauses describing the age of the human, “he knows or has reason to believe is less than 15 years of age.” The plain language and clear intent of the General Assembly is to protect solicitation of a live human, not solicitation of a cartoon. “Where a statute is unambiguous, the plain meaning is to be accepted without resort to the rules of statutory

interpretation.” *Last v. Virginia State Board of Medicine*, 14 Va. App. 906 (1992). If the General Assembly intended to allow for imaginary people, it might have written the statute:

*Soliciting ... any person or imaginary person he knows or has reason to believe is younger than 15 years*

*Soliciting ... any person, real or imaginary, he knows or has reason to believe is younger than 15 years*

There is no crime under Va. Code § 18.2-374.3 for soliciting an adult, imaginary person, or cartoon.

#### **E. Interpreting Va. Code § 18.2-374.3 as Subordinate to § 19.2-61, *et seq.***

Va. Code § 18.2-374.3 was passed in 1992. It was not derived from federal statutes. Nevertheless, it deals with communications covered under ECPA. It should be read as a subset of the older § 19.2-62 or be subordinated to it. Interpretations of § 18.2-374.3 have failed to consider § 19.2-62, but § 18.2-374.3 can only be fully understood in conjunction with § 19.2-62 and its federal equivalent 18 U.S.C. § 2511. *See Crislip v. Commonwealth*, 37 Va. App. 66, 71-72, 554 S.E.2d 96, 98-99 (2001).

The key phrase “has reason to believe,” exists in § 18.2-374.3 but does not in § 19.2-62. Bauer cannot be ‘such person’ and ‘party to the conversation’ pursuant to § 19.2-62, while simultaneously claiming he is Alex VA shown in the picture, pursuant to § 18.2-374.3. If the court concludes that Bauer impermissibly intercepted communications (pursuant to § 19.2-62 *seq.*) and Achin’s rights were violated, then the § 18.2-374.3 charge cannot stand.

#### **F. Using a Phone as an Interception Device**

Online sting operations sometimes feature undercover officers trolling on dating sites using their phone (or computers) without a warrant. *See Appendix 16 at 5:22-16:1*. Many sites have user

agreements expressly prohibiting this practice. Grindr's User Agreement, July 1, 2018 (*Appendix 14*) states:

- You must be a legal adult. You hereby affirm and warrant that you are currently eighteen (18) years of age or over (twenty-one (21) years in places where eighteen (18) years is not the age of majority) and you are capable of lawfully entering into and performing all the obligations set forth in this agreement. (at 2 sec. 1.2)
- You will NOT impersonate any person or entity, falsely (at 5 sec. 8.3.7)
- Government End Users. The Grindr Services are intended for the use by individuals, not government entities.... Otherwise, nothing in this Agreement or otherwise will give a government user rights to the Grindr Services broader than those set forth in this Agreement. (at 12 sec. 15.8)

Grindr strictly enforces these policies. Achin reported the underage user to the Grindr system administrator. Bauer's fake account was quickly suspended. *See Appendix 16 at 18:11-13.*

A *user* is defined as "any person duly authorized by the provider to engage such use." Va. Code § 19.2-61, Md. Code § 10-401(17), and 18 U.S.C. § 2510 (13)(b). Since Bauer violated this user agreement, he was not duly authorized to use Grindr. Once thrown off, Bauer established a new account to pursue Achin, tricking Grindr via a new persona "Alex" signified by a male bathroom icon as the profile image (R. at 000872). The Grindr application is installed and becomes a component of the phone. Because Bauer was not lawfully using Grindr in "ordinary course of business," his phone became an interception device to obtain communication content. *See* Va. Code § 19.2-61.

### **G. Reverse Targeting of U.S. Citizens**

Police misuse of technology is a domestic version of "reverse targeting" (indirect targeting) against U.S. citizens.

The Foreign Intelligence Surveillance Act of 1978, Amendments Act of 2008 (FISA) extended Fourth Amendment protections to U.S. persons when they are on foreign soil and when they communicate with foreigners. However, Fourth Amendment protections do not extend to foreigners on foreign soil – they can be monitored. FISA strictly prohibits collecting communications of non-U.S. persons for an ulterior motive, such as intercepting their conversations for the purpose of recording their true target, a U.S. person. Section 702 of the FISA Amendments Act of 2008 outlines the distinction. *See also* 50 U.S.C. § 1881a (b)(2) and *Appendix 11 at 24-25*:

*Who can't be targeted • A foreign person located abroad for the purpose of targeting a U.S. person or person inside the U.S. with whom the foreign person is communicating (often called "reverse targeting" or "indirect targeting")*

*"Reverse targeting," the targeting of a U.S. person under the guise or pretext of targeting a foreigner, is expressly prohibited.*

Police have adapted their investigative techniques to include such targeting. In the process they inadvertently or directly violate the law. Detectives create imaginary people who have no Constitutional rights. Police then target communications of imaginary people solely to intercept communications exchanged with their true target, a U.S. Person. These actions are "reverse targeting," domestic style. They cross the line of legitimate police investigative work for they actually target persons and trounce one's Constitutional protections.

## **H. Electronic Warfare against U.S. Citizens**

Sting operations conducted in this fashion meet the federal government's technical definition of electronic warfare against U.S. citizens.

Signals received by a cell phone are electronic magnetic (EM) spectrum signals (EMS). Signals transmitted over an internet wire connected to a computer are EMS signals as well. Military and intelligence personnel may transmit a signal or send communications to better surveil the target. This is only allowable if the target treats it as background ambient noise (e.g. shining a flashlight, radar, sonar, or spam email). When a deceptive transmission leads the target to react in a manner detrimental to itself, however, the transmission has crossed the ambient noise threshold and is now considered an act of electronic warfare (EW). *See Joint Publication 3-13.1 Electronic Warfare (2012), Appendix 7:*

*Electronic Attack: Use of EM energy to attack personnel with the intent of degrading or destroying enemy combat capabilities. (page viii)*

*Principle EW Activities: Include EM deception and electronic masking. (page viii, I-7, I-8, I-13)*

*EW Role in Information Operations: Includes offensive tactics to shape and exploit adversarial use of EMS, including wireless telephone (page ix, I-14)*

*EW Role in Cyberspace Operations: Since cyberspace requires both wired and wireless links to transport information, offensive cyberspace operations may require use of the EMS for the enabling of effects in cyberspace (computer network operations) (page ix, I-15,16)*

Hypothetically, let's suppose a DoD employee figured out how to clone a Russian officer's phone. Employee obtained authorization to impersonate the Russian officer and transmit a message to Russian troops requesting a photo of their battle plans. Employee has launched an electronic warfare attack. Should the transmission cause a reaction resulting in the battle plan photo sent in reply, the electronic warfare attack would have been successfully carried out.

In our domestic example, Bauer sent communications to Achin, masked to look like it came from a trusted source, "Alex VA." Bauer transmitted a deceptive message with a picture of someone else (using an EMS signal) to Achin's electronic device (launching an electronic warfare attack). Achin answered this communication in a manner ultimately detrimental to himself. He


was arrested. Bauer’s electronic warfare attack was successfully carried out. Using electronic communications in this manner crosses the line of legitimate police investigative work.

### 5.3 Searching Computers and Electronic Devices

#### A. Searching a Confiscated Device

A confiscated phone should be placed in a Faraday box (or equivalent) to prevent sending or receiving communications. This preserves the integrity of evidence. Received messages are stored in finite, recycled phone memory. New messages would overwrite data that may contain important evidence. Activating “airplane” mode on a phone prevents transmissions. It does not prevent receiving messages, updates, or “erase everything” commands. Each phone application handles airplane mode differently; it may or may not process received communications.



This picture from discovery shows Achin’s phone on a table, not in a Faraday box. It was not in airplane mode . It did have 13 new messages, Google voice command activated, and a live weather report. The phone was modified as the background photo of Achin’s daughter was no longer shown (per Achin). The integrity of this phone in evidence was thereby compromised.

IMG\_0386 (following IMG\_0385, R. at 000896)

A defendant needs access to his seized electronics to perform forensic analysis. In *Commonwealth v. Hawthorne*, the computer was released from evidence 19 days after Hawthorne’s arrest by order of the arresting detective. Its memory was erased, unbeknownst to

Hawthorne. *See Appendix 12 at 3.* Yet, 3 months later, Court was informed the computer was “still being analyzed.” *Appendix 12 at 1.* Defense’s forensic expert never saw the computer. Unaware of this Brady violation, defense counsel advised Hawthorne to accept a plea deal. How can police do this without consequence?

## **B. Hash Codes Identifying Content**

Police use varied technologies in their investigations. For example, Shareaza-LE (available only to Law Enforcement) allows detectives to remotely search devices. It is a more powerful version of Shareaza, a commercially available peer-to-peer file (P2P) transfer product. Shareaza uses hash codes as part of its internal file transfer mechanism. Bauer explained hash codes during his interrogation of Achin. *See Appendix 15 at 03 (101:7-23).*

The hash code is a unique number calculated from a computer file’s content using a set formula. Hash codes are designed to “verify that a completed downloaded file has been correctly transmitted.” *See Shareaza User’s Manual (online) (Feb. 2, 2014), Appendix 8 at 25.* If the hash code computed after transmission does not match the original, a transmission error has occurred and the file must be retransmitted. The hash code algorithm I wrote for GTE computed a file’s hash code and attached it to the file sent. Upon successful receipt of the file, that hash code was removed and discarded.

Brand new computers do not have hash code calculators, but peer-to-peer file transfer program (like Shareaza) do have them to validate transmissions. Since computing hash codes takes time, some programs pre-calculate and store hash codes. In Shareaza, hash codes are not just calculated for files transmitted, but “Shareaza looks at all your files, creates a checksum [hash code] for them and puts them in the correct category in your library.” *Appendix 8 at 13, #2.*

(emphasis added). This feature not only calculates hash codes for files transmitted but also for one's private files, even if they are never sent.

Bauer showed he understood this practice saying, "with technology, everything is given a very specific hash." *Appendix 15 at 03 (101:7-8)*. As the user creates or modifies files, Shareaza updates this library. As Bauer explained, "your conversation when stored will have a hash. The photo you took will have a hash. Everything does." *Appendix 15 at 03 (101:8-10)*. Peer-to-peer users must explicitly exclude files they do not wish shared by entering a file extension "and click add." Otherwise everything on one's computer is shared. *See Appendix 8 at 19*. Users are told they have to "allow others to browse shares" in their library, because "turning off this feature hurts the community. It offers no real extra security by turning it off." *Appendix 8 at 18, bottom*. Bauer made it clear, "And this is not public knowledge." *See Appendix 15 at 04 (102:6-8)*.

Bauer's description of hash codes mirrors that of Det. Brisentine (*Commonwealth v. Lopez* (Amelia County, 2016)), who described hash codes as a "fingerprint." *Appendix 10 at 54:5-11* and *Appendix 15 at 03-04 (101:19-102:1)*. This is because police routinely glean hash codes to populate a database, which maintains a content inventory of citizens' personal computers. *See Appendix 10 at 52:25-53:12*. No warrant was obtained to glean this data. Since hash codes derive from content, they are subject to Va. Code § 19.2-62 and / or 18 U.S.C. § 2701. Police admission that hash codes catalog and "fingerprint" content of private computers into a police database without any warrant, is chilling.

### **C. Hash Codes are Protected by the Stored Communication Law**

Hash codes are designed to validate transmission of file pieces as they are stored, forwarded, and stored again. They are protected by Stored Communication Law. Hash codes are NOT intended as an inventory tag for cataloging private content, as Bauer and Brisentine



understood police usage. Whenever law enforcement uses a communication application for a purpose outside its design, they are “exceeding the authority granted to them.”

18 U.S.C. § 2701 - *Unlawful access to stored communications:*

*(a) OFFENSE.—Except as provided in subsection (c) of this section whoever—  
(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or  
(2) intentionally exceeds an authorization to access that facility;  
and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system ... (emphasis added)*

File transfer programs are built by software engineers, installed on computers, and are established to serve a particular purpose. Merriam-Webster’s (2019) defines this as “facility: *something that is built, installed, or established to serve a particular purpose.*” See “facility” as used in Va. Code § 19.2-61 *et seq.*

People are familiar with network service providers, like Verizon, that transfer emails and electronic files. When sending a file, it is first forwarded to Verizon, which stores then forwards it in a continuous chain until it reaches the destined computer. While files are being stored and waiting to be forwarded, private content contained within is protected by the ECPA Stored Communication Act 18 U.S.C. § 2701. Police need a warrant to gain access to files while being temporarily stored at Verizon.

Commercial-grade peer-to-peer file sharing programs are used to distribute larger files to many customers. These programs are installed on one’s computer. See *Appendix 10* at 48:3-5. Most commercial file sharing products are based on the BitTorrent protocol. BitTorrent’s website claims its products carry 40% of the world’s internet traffic daily. See *BitTorrent Usage* (January 2020), *Appendix 19*. Facebook and Twitter utilize BitTorrent to distribute updates to their servers. Universities use it to distribute large datasets. Large files are chopped into smaller pieces for ease of transmission, then reassembled in the destined computer.

Commercial file sharing programs like Shareaza have virtually no file storage of their own. Instead, Shareaza creates a folder on the user's disk drive to store file pieces being sent or received. The user agrees to "share" disk space on his computer disk with the service provider, granting storage for file pieces. Once the complete set of pieces have been received, the file is assembled and provided to the user as a finished communication. File pieces are stored communications and useless as individual units. Only when reassembled does the file become usable. Pieces are stored in folders by Shareaza to satisfy future transmission requests of other Shareaza customers. Both the stored communications (file pieces) and the delivered communication (assembled file) are located in the user's computer in his home, protected by the user's username / password. The "location of the evidence" is critical when answering Fourth Amendment questions. *See Appendix 3 at 52 bottom, 75-76.*

1. Is government action involved? YES
2. Does the person affected have a reasonable expectation of privacy in the place or thing to be searched? YES

When a user makes a request, he grants limited access to his computer via a special inbound address (port number) for the sole purpose of transferring files and pieces, e.g. Shareaza "default [port] is 6346." *Appendix 8 at 20.* Microsoft Windows-10 uses its BitTorrent-style peer-to-peer file sharing program by default to "get updates from and send updates to other PCs." See Microsoft Windows 10 BitTorrent (December 18, 2018), *Appendix 17 at 2 (bottom) and 5 (bottom)*. The files downloaded to one's computer are "shared" with other Windows-10 users. Granting Microsoft special access at port 80 to deliver Windows-10 updates is akin to Shareaza's special access at port 6345 to deliver files. In each case, the agreement is between the user and the commercial vender, not between the user and other users of the product. Both Windows-10 and Shareaza maintain the anonymity of users. Files are still private and inaccessible to the public.

How can one have “no reasonable expectation of privacy that the Fourth Amendment will protect” him when merely enabling peer-to-peer capability to update Windows-10? See *U.S. v. Perrine*, 518 F.3d 1196 (10th Cir. 2008).

Partial file pieces awaiting assembly figured prominently in the Lopez case. They were downloaded from Lopez’s computer without a warrant by Brisentine (*see Appendix 10 at 51:14-52:1, 52:20-24, 53:13-22*) from a specific IP address (*see Appendix 10 at 49:11-14 and 52:13-14*), a capability unavailable to the general public. See 18 U.S.C. § 2701.

Both Shareaza and Shareaza-LE can only communicate with computers having a BitTorrent-based file sharing application installed (e.g. Ares, *See Appendix 10 at 48:17-24*).

“Shareaza le is designed to allow access to any shareaza user's file system without their knowledge, and to permit stealth downloading of any files found. It is like the police having a skeleton key that gives access to your house and property anytime at will.”  
*Appendix 8 at 31, 22:53 entry.*

Police can remotely access a computer without having to answer username / password questions. Police then have access to content stored on that computer. Shareaza-LE creates a 2-way portal into that device, allowing the officer to inventory, remove, or deposit files - all without the owner’s knowledge or consent. Since Shareaza stores hash codes for “all your files” in its library, an officer:

“might have access to your entire hard drive, and be able to retrieve personal information that might be used against you. Also, if the aim is entrapment, there is no reason to believe that illegal files will not be planted on your computer.”  
*Appendix 8 at 31, 23:30 entry.*

#### **D. Hash Codes used to Populate the Database and Send Notifications**

File pieces must be managed so the requested file can be reassembled. A torrent file is an inventory of file pieces. *See Appendix 8 at 27.* This torrent file includes filenames, size, a hash code for each piece, and a web address of the file's "tracker." The tracker file logs hash codes derived from content AND transactional records, i.e. IP address locations where pieces have been stored so they can be retrieved to satisfy future requests. *See Appendix 8 at 27.* Although tracker files are on the internet, they are not human readable. They are only written and read by a BitTorrent compatible program which deciphers the content.

Brisentine testified that the database (*see Appendix 10 at 53:12*) contains filenames (*ibid. 49:20-50:7*), hash codes (*ibid. 54:1-11*), IP address locations of private devices (*ibid. 49:9, 50:8-14*), and subscriber identification (*ibid. 50:11-18*), all gleaned before he "contacted the local jurisdiction" or obtained subpoenas / warrants. This implies the database catalogs IP addresses by subscriber (name and home address) and inventories private content (tagged by hash code) of unsuspecting citizens' locked computers. This inadvertent admission raises questions. It suggests a law-enforcement-only tool exists that regularly scours internal tracker files and populates a database with transactional records. This tool is possibly Torrential Downpour. *See U.S. v. Hoeffener.* When "law-enforcement-only" tools are necessary to extract information from a tracker file, it is not "publicly available."

**Publicly Available** - The information must be available to any member of the general public.

*See Office of Director of National Intelligence (DNI), Civil Liberties and Privacy Guidance for Intelligence Community Professionals: Properly Obtaining and Using Publicly Available Information (July 2011), (Appendix 6 at 3 #1).*

Accessing tracker files to derive content (hash codes) and transactional records (IP addresses) without a warrant exceeds authorization to access the internal workings of a file-sharing facility. *See* U.S.C § 2701.

Although most subscriber information requires a subpoena, obtaining IP addresses from transmissions (transactional records) requires a search warrant. *See Appendix 3 at 78-79*. Neither subpoena nor warrant was obtained. Since Lopez’s computer used Ares, not Shareaza (*Appendix 10 at 48:22*), whatever tool the police used has Shareaza-like capability to interface with other peer-to-peers (P2P) networks. *See Appendix 8 at 4*.

According to Brisentine, Shareaza-LE’s suite of tools have other capabilities as well. As new information is obtained and the database updated, it is cross-referenced for “known or suspected child pornography.” *Appendix 10 at 49:8-11*. If found, the appropriate law enforcement agency is identified and contacted since “every user’s ip address [is] mapped to a city and street,” and “every file that you exchange can be traced back to you.” *Appendix 8 at 32, entry 22:53*. Yet geo-location for identification requires a warrant. Va. Code § 19.2-70.1-3. No such warrant was obtained. *See U.S. v. Jones*, 565 U.S. 400 (2012). Torrential Downpour-like database entries require a corresponding Warrant ID field, indicating proper legal authority was obtained. **This Warrant ID field appears missing from the database.**

An automated search for pornography appears to have been done on Achin’s phone, given the speed by which the search was completed while Achin was being interrogated. (R. at 000331(99:3-5), 000444(212:18-19)). Searching for child pornography was the stated reason for obtaining a search warrant of Achin’s home, but none was found. (R. at 000328-000329)

## E. Remotely Searching Computers

In *Commonwealth v. Lopez*, Brisentine testified that after the hash code database tool flags an IP address, he identifies the subscriber from the IP address using law enforcement's database without obtaining a pen register warrant. *See Appendix 10 at 50:11-14 and Va. Code § 19.2-70.2.* Brisentine then used Shareaza-LE to remotely tunnel into Lopez's computer and download files. No warrant was obtained until after he had completed his search and downloaded content. *See Appendix 10 at 52:20-53:22.* Brisentine re-confirmed he downloaded filenames, partial files, and entire files prior to obtaining a search warrant. *Ibid. 56:1-9.*

“...while you are using shareaza, unbeknownst to you, a cop could be scrutinizing all your files, whether you have shareaza set to allow viewing of shares or not.”  
*Appendix 8 at 31, 23:30 entry.*

As a network engineer, I identified three main ways to gain remote entry into a device via internet:

1. No username / password– public access or non-sophisticated private user
2. Username / password – provide valid credentials to gain entry
3. Backdoor – used by commercial tools to provide specific updates and services, or law enforcement's surreptitious use.

When a detective remotely breaks into a private computer to search its content, and that computer has a username / password, a warrant is required. Private computers are typically stored in a home or business behind a locked door. Brisentine conducted an “examination of the interior of property by technical means,” 50 U.S.C. § 1821. Even using a thermal imaging device to scan a home's exterior constitutes a search requiring a warrant. *See Kyllo v. United States*, 533 U.S. 27 (2001).

Distinguish between public and private file access is important. Ignorance can confuse judges or lose cases. *See Oregon v. Combest*, 350 P. 3d 222 - 2015; *also U.S. v. Hoeffener*. Although Combest's defense argued that his computer was searched without a warrant, he failed to argue that the files in question were indeed private files (not public), thus requiring a search warrant. Combest also failed to argue that hash codes used in a database constructed to inventory content of one's private computer violates 18 U.S.C. § 2701.

Law enforcement claims that user's Shareaza files are "shared," therefore "public." They argue detectives don't need a search warrant for devices at an IP address using Shareaza-LE. However, files cannot not be retrieved by the general public from a specific IP address using Shareaza or any other public tool. Only Shareaza-LE (law enforcement only) could retrieve the files, so the files were **not** "publicly available." A warrant was required, but never obtained.

Dropbox is an example of another category of file sharing applications Law Enforcement uses. Here files are shared amongst a limited group of users, but not the general public. The user who creates a Dropbox becomes its administrator. He deposits a file in his Dropbox, then sends his Dropbox link to another person(s), who is the intended recipient(s). When the intended recipient(s) accesses a file in the Dropbox, it causes the file to transfer directly from the sender's computer to the recipient's.

Unlike Dropbox, users of Shareaza-like programs remain anonymous and cannot copy anything from a specific user. The user contacts the service provider, Shareaza, NOT another user. The Shareaza application determines which other anonymous computers have the requested file pieces, transfers them to the requesting user, and reassembles the completed file. These users have no idea what file pieces remain on their computer or were copied off their machine.

As a system administrator (*see Appendix 2 at 1-2*), I copy files directly from IP addresses. I enter “copy”, an IP address, directory, and the filename. The system immediately prompts for a username / password and requires a valid response. Additionally, I am not allowed to download filenames or content unrelated to my job. When law enforcement uses applications not available to the general public, or bypasses username / password on private devices, they are “exceeding the authority granted to them.” 18 U.S.C. § 2701.

If being a government employee can open doors that are close by law, policy or practice to members of the general public, the information sought is not “publicly available.”  
*Appendix 6 at 4 ¶6.*

If the user’s Shareaza files were truly “public,” then a system administrator (like myself) could “copy” these files without any special tools or authorization. Such authorization was bypassed in *Commonwealth v. Lopez*. Detectives used Shareaza-LE to enter the computer via the backdoor Shareaza port – not through the front door with a username / password. This backdoor Shareaza port only answers to a special electronic “key” used by file-sharing programs like Shareaza. Shareaza-LE imitates the electronic “key” necessary to communicate with Shareaza, allowing detectives access into a private computer. Therefore, the user’s Shareaza files were private, not public, and required a search warrant to obtain them remotely. A search warrant was never obtained, however.

#### **F. User Errors Affected by Hash Codes and Third-Party Malicious Intent**

Bauer stated, “The photo you took will have a hash. Everything does. If anything is changed – that would all change.” *Appendix 15 at 03 (101:9-12)*. While perhaps true for police, it is not true for software programmers. BitTorrent files resemble this hard-copy brief, having pages, a table of contents, and a binding. If anyone used ink or white-out on one page in this brief, it

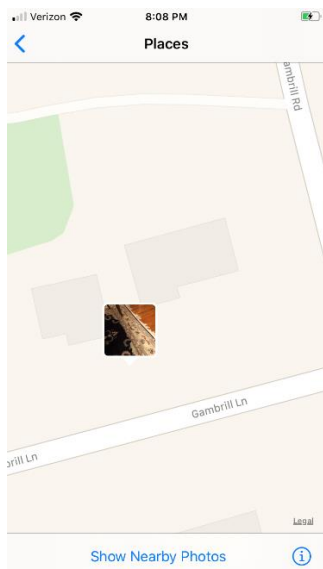


would be visible and detected. Similarly, a hash code is calculated to detect errors on one page (e.g. half megabyte) of a large file. This brief is securely bound to prevent pages from being replaced or added. The file binding for BitTorrent is similar to the binding of a loose-leaf notebook. Pages are received in random order from multiple computers and reassembled in something resembling a loose-leaf notebook. A software programmer can even replace or add pages. The table of contents can be updated to reflect changes. From my analysis of the BitTorrent design, there is no hash code certifying the table of contents ever changed. Their design simply corrected transmissions errors, it did not detect malicious changes to files. Seemingly innocent files could have “pages” of illegal content substituted or added, unbeknownst to the user downloading it. Such malicious action could sow doubt of “intent” for the accused and impinges on whether this defendant “knowingly possesses” inculpatory file pieces. *See* Va. Code § 18.2-374.1:1.

If a user mistakenly selects a file to download from a file sharing service, then interrupts the download and deletes it, the corresponding transactional record (though accessed in error) remains permanently logged. This is because the IP address is permanently linked to hash codes in the tracker file. No user can correct the tracker file since it is not “publicly available.” If a police tool scours the tracker files for IP addresses and hash codes, it would trigger an alert. Some file pieces may even have successfully transferred. Police using Shareaza-LE will find potentially inculpatory file pieces where the innocent user thought he successfully interrupted the mistaken transfer.

## G. Geo-location via Photographs

Bauer stated, “If you took a photo, ... it will say ... the type of phone. Sometimes it will give you location.” *Appendix 15 at 03 (101:12-16)*. Photos taken by a smart phone can be tagged with latitude and longitude (lat/lon) indicating where the photo was taken.



This data is precise enough to locate the phone within a few houses, sometimes even a specific room. See map (left) tagging me within 30 feet. Photos are often embedded within private messages and are intercepted by police during online sting operations. These photos (including tags) are protected by ECPA, but the lat/lon could easily be used by police to locate the suspect. As geographic tags come from the cell phone’s own GPS, utilizing such tags to geo-locate a suspect may require a warrant. *See U.S. v. Jones*, 565 U.S. 400 (2012) and *U.S. v. Katzin*, No. 12-2548 (3d Cir. 2013).

## 5.4 Authority Expressly Granted to Intercept

Both Federal and Virginia Electronic Communications and Privacy (ECP) law detail a specific list of authorized persons who may intercept communications and precise methods they may use. All other interception is illegal. Va. Code § 19.2-62(B)(1) grants interception rights to employees of electronic service providers, who may perform random intercepts and monitor communications in the course of their duties. System administrators who abuse this authority have been prosecuted. *See U.S. v. Polequaptewa*, (8:16-cr-00036 District court, D.D. Calif. 2018). Virginia General Assembly specified that only Virginia State Police officers can intercept and

monitor under carefully controlled circumstances and with Court approval. Va. Code § 19.2-68(C)(4).

Another provision in the law defines who may be party to the intercepted communications. Unlike Virginia, some states (Ohio) and Federal statutes expressly provide that law enforcement officers are party to communication (18 U.S.C. § 2511(2)(C)):

*It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.*

Va. Code § 19.2-62 is more restrictive, however. It does not allow law enforcement as party to communications. Neither Federal nor Virginia statutes grant police authorization to impersonate someone else in any electronic, oral, or wire communications – even with permission.

Logically, if a phone operator or network engineer cannot legally impersonate or create an imaginary person to intercept communications of someone, then police cannot impersonate or create imaginary people to do that, either. Virginia law specifically denies law enforcement such authorization, yet this denial is universally ignored.

### **5.5 Question for the Court: Does Va. Code § 18.2-374.3 Criminalize Teen Dating?**

Sixteen is the age of consent to marry in Virginia. Va. Code § 18.2-374.3’s “seven years older” clause attempts to differentiate criminal solicitation from legitimate dating. However, this clause only appears in the penalty section of the statute, not when defining a crime itself. This omission effectively codifies as felonious dating communications between 17 and 18-year-olds.

If a young adult communicates with a minor online and the conversation turns risqué, he is often found guilty of soliciting that minor. Period. Witalec was 17-years-old when he exchanged private messages with his 15-year-old girlfriend in a nearby school. *See*

*Commonwealth v. Witalec* (Stafford County, 2016). Both were never in the same room (this younger generation considers online dating normal). The girl took pictures of herself clothed in a T-shirt and panties and sent them to Witalec. After Witalec turned 18, continued communications became felonies. He was charged with 20 felonies and faced 350 years in prison. Sending dating messages was deemed “lewd and lascivious intent,” irrespective of context or their relationship status. Under Va. Code § 18.2-374.3, an 18-year-old discussing the wedding night with his 16-year-old fiancée is felonious, punishable by 5-30 years in prison. Such discussions are even considered a violent sexual offense, earning one 25 years on Virginia’s sex offender’s registry upon release. Sending private photos attired in intimate apparel is an additional felony for child pornography.

§ 18.2-374.3

*(B) It is unlawful for any person to use a communications system... for the purposes of procuring a minor for any activity in violation of 18.2-374.1. A violation of this subsection is a Class 6 felony.*

*(C) It is unlawful for any person 18 years of age or older to use a communications system for the purposes of soliciting, with lascivious intent, any person he knows or has reason to believe is a child younger than 15 years of age ... is guilty of a Class 5 felony.*

*(E) Any person 18 years of age or older ... soliciting any person he knows or has reason to believe is a child younger than 18 years of age...is guilty of a Class 5 felony.*

Provisions of Va. Code § 18.2-374.3 mirror the same provisions in the Computer Decency Act of 1996 (CDA) which was partially ruled unconstitutional under the First Amendment. “In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another.” *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997). The *Reno* ruling also invalidated a CDA provision imposing criminal penalties for transmission of “indecent” materials to a person known to be under 18 as violative of the First Amendment.

The Declaration of Independence declares “that all men are created equal, that they are endowed by their Creator with certain inalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.” What greater example of personal liberty can there be than the freedom to date and choose one’s spouse? By codifying dating as a felony, this statute further violates the Fourteenth Amendment. "Their right to liberty under the Due Process Clause gives them the full right to engage in their conduct without intervention of the government," wrote Supreme Court Justice Kennedy. *See Lawrence v. Texas*, 539 U.S. 558 (2003).

## **6. Conclusion**

The power granted to me by such erroneous precedents is jaw-dropping. If no warrant is required to access and retrieve transactional records from the internal BitTorrent tracker files, then engineers like me can download the free BitTorrent source code from the reputable Sourceforge.net website. We would be legally permitted to create our own database inventorying the content of people’s private computers. Engineers like me could also download our own free copy of Shareaza source code to write a customized Shareaza-Bonnie version. Engineers like me could use Shareaza-Bonnie to remotely enter other citizens’ computers at will to obtain anyone else’s file listings and file content, including computers having Shareaza-LE. This data can then be publicly sold for profit by private companies (like Blue Ridge Software Consulting). Should using law-enforcement only tools like Shareaza-LE and Torrential Downpour require a warrant to protect one’s privacy? It should.

In fact, Va. Code § 19.2-62(B)(1) grants more authority to operators and network engineers at a telephone company to intercept communications than Virginia statutes grant to police. If the local police can impersonate others to intercept communications, then why can’t service providers

to do the same? If local police can control imaginary people online to intercept private dating communications, can't Google engineers do that too? If the police can disclose private conversations to the Court and press, can't a network engineer do the same? If phone employees can't legally do this, the police can't either.

If the Court disagrees with my arguments on interception, then police can, with no color of law exception or warrant:

- combine multiple images, voice, and texting to animate life-like images that speak and text. The person depicted in the image may be real, partially-real, or a cartoon. Their likeness and a manufactured voice could be used to intercept communications for they would be lawful parties to any communication, a legal impossibility under current law.
- manipulate imaginary people to entice someone to commit a crime.
- take the “faithless friend doctrine” to new level. Someone authorizes his/her image for innocent use. Police in turn manipulate this person’s voice and image to say and do whatever the police type into the keyboard. They record the “friend’s” conversation with another, press charges, and release it to media, claiming the right because they are law enforcement and “a person and such person is party to the conversation.” Where does it end?
- can bypass usernames and passwords to remotely enter any private computer or electronic device. They can freely inventory what is on the computer, download files and other content.

If the Court agrees with any of my arguments, then:

- The basic principle remains strong: a “person” is defined as **one** human being capable of having rights and has only **one** birth certificate.

- Constitutional protections remain intact. People have a right to privacy in private conversations. People have a right to be secure in their house and effects (like computers) against unreasonable remote searches and seizures.
- Law enforcement must obtain a warrant to circumvent these basic Constitutional principles that have been upheld in Courts.
- Evidence obtained in violation of ECPA and evidence derived therefrom should be suppressed. *See* Va. Code § 19.2-65 and 18 U.S.C. § 2515. Charges should be dismissed accordingly.

Det. Bauer testified that he never received any training on the ECPA, and he was not familiar with it. *See Appendix 16 at 22:20-23:3*. This is in marked contrast to extensive training required at the federal level. *See Appendix 2*. Ignorance of the law is no excuse, even for law enforcement and those who advise them. Qualified immunity should not apply since these operations and resulting prosecutions violated federal and Virginia statutes from the outset. The Virginia Attorney General is charged with enforcing these laws, but took no action when I reported violations. *See Appendix 13*. The public has been convinced that sting operations using imaginary people are necessary before a real child is harmed. The ends justify the means. It should be the responsibility of law enforcement to catch criminals, not manufacture them.

It is requested that the Court order the investigation of ECPA statute violations identified in this brief, prosecute as is appropriate, and exonerate those illegally prosecuted.

Respectfully submitted,

---

Bonnie Burkhardt, *Pro Se*  
8402 Gambrill Lane  
Springfield, VA 22153  
Phone: (703)505-2793  
Email: [Bonnie.burkhardt@blueridge-sw.com](mailto:Bonnie.burkhardt@blueridge-sw.com)

Dated: March 17, 2020