VIRGINIA:

IN THE APPELLATE COURT
OF VIRGINIA

COMMONWEALTH OF VIRGINIA	)	
	)	CAV RECORD NO. 1945-19-2
v.	)	
	)	HANOVER COUNTY CIRCUIT COURT
RYAN PICK	)	CASE NO. CR18001081-00 thru -02
Defendant	)	
	)	

***AMICUS CURIAE* BRIEF FROM BONNIE BURKHARDT**
IN SUPPORT OF DEFENDANT RYAN PICK

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

1. Table of Contents

2. Table of Authorities

Cases

Statutes

Other Authorities

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 professional network protocol 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 text messages and private messages exchanged over the internet, 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 these laws and the police tactics used in these cases. 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. Cell phones provide TDD/TTY via text messages. Americans with Disabilities Act (1990) codified 47 U.S.C. § 225.

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 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 derived 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), *and See 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 10, 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.* (R. at 72 ¶5).

4.2 Issues Before the Court

First Issue - The Court erred when it denied Defendant Ryan Pick's Motion to Suppress Internet Chats and evidence derived therefrom.

If this was a picture of 48-year-old Det. Troy Payne dressed in disguise and calling himself as "Lilly," Payne would have been party to the Omegle conversations. That did not happen.

(R. at 649)

The Court erred because the female pictured, Lilly, was not party to any electronic communications, though she was the intended recipient. There is a distinction to be made between being a participant in a conversation, and being a person party to a conversation. Robo callers participate in conversations, but cannot record unless they make a disclaimer. They are not "such person," party to the conversation. Payne likewise was a participant, not a lawful party to the conversation since he impersonated "such person" pictured in the photo. *See Appendix 17 at 8:14-22.*

The common analogy of a football pass interception explains a wiretap, but not the interception of this case. *See Appendix 17 at 5:3-13.* The Court erred by taking a position that "some other means is being used to intercept the communications" as the complete definition of an illegal "intercept," even though the ECPA expanded the meaning. *See Appendix 17 at 17:15-18 and 17:19-19:14.* "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." *See* Va. Code § 19.2-61 and 18 U.S.C. § 2510.

In *U.S. v. Szymuszkiewicz,* — F.3d —, 2010 WL 3503506 (7th Cir. September 9, 2010), Szymuszkiewicz was convicted for being a recipient, but not the intended recipient, of emails sent to his boss. Szymuszkiewicz was a system administrator who had secretly setup auto-forwarding on his boss's email account so copies of emails would 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 (like Payne did). Old-fashioned wiretaps are not the only way to intercept communications.

The Prosecution said "Lilly is not a real person, is imaginary." *See Appendix 17 at 9:15-16.* Imaginary people and cartoons cannot legally authorize anything, like the interception and recording of a conversation. The female pictured was not party to any conversation. Payne "cannot pretend to be the person" Lilly. *See Appendix 17 at 7:20-22.* Payne intercepted the cell phone transmission and message content; the female never received them. *See* 50 U.S.C. § 1801(f)(3).

There was no probable cause for Payne to be on the chat site Omegle investigating a crime. Payne "did not know who Ryan Pick was when he began this chat" with a random stranger. *See Appendix 17 at 10:4-19.* Interception and recording began with a Stranger saying, "Hi" on Omegle. *See Appendix 19 at 19 (109:5).* What probable cause exists after uttering "hello" that would permit interception and recording of a private conversation between "Stranger" calling

himself "Ryan," and "Lilly"? None. Prosecution specifically stated, "this was not an investigation into Ryan Pick specifically." *See Appendix 17 at 10:2-3.*

Evidence provided was intercepted content of private text communications. Both state and federal law allow a person to intercept his own conversation. There is no provision for impersonators or imaginary people to intercept as *"such person is a party to the conversation*" cannot be satisfied. If Payne was impersonating Lilly in the photo, then Payne was not "such person" who was party to the conversation. If Lilly is an imaginary person created and controlled by Payne and imaginary people don't really exist, then the law does not protect imaginary people. Lilly has no legal standing. Not only is unauthorized interception a felony and a federal crime, but also any "endeavor to intercept." *See* Va. Code § 19.2-62(A)(1) *and* 18 U.S.C. § 2511 (1)(a).

The defendant's motion to suppress evidence should be granted on the grounds that there was no legally obtained evidence. Payne intercepted communications intended for Lilly in violation of Va. Code § 19.2-65 and 18 U.S.C. § 2515. These intercepted communications formed the basis of the evidence against Pick and should be suppressed, the charges against Ryan Pick dropped.

Second Issue - The Court erred in allowing unlawful identification of Ryan Pick as the suspect.

Identification was achieved not only from the intercepted content, but also from interception of private electronic routing information and location data. Payne obtained the suspect's name, "Ryan Pick," on July 10th by doing a Google search using the town name, "Woodbridge." *See Appendix 13 at 10¶2.* The term "Woodbridge" was not in the Omegle

conversation transcript. *See Appendix 13 at 3-10 and Appendix 19 at 19-29.* On July 10th, the only possible source of the term "Woodbridge" would be from the underlying Dropbox network routing information, which police obtained without a pen register warrant. *See* Va. Code § 19.2-70(1-3) *and Appendix 3 at 26*. That same day, Payne researched the user's full name, home address, and place of work prior to writing any warrants or subpoenas.

Google search terms "Ryan," "music teacher," and Snapchat account "stonynots," were obtained from the Omegle chat content without a warrant. There is nothing tying these terms to a specific Omegle user, since anyone could type it. No Snapchat communication occurred between "stonynots" and Payne. There was no warrant to identify the anonymous user from content or from underlying network routing information.

Defense argued this police sting operation violated Va. Code § 19.2-61, *et seq*, which also defines "pen register." *See Appendix 17 at 3:19-23.* In addition to these statutes regulating access to the private communications, the "pen register" portion of these statutes regulate obtaining information from the underlying transmission path used, such as geo-locating the transmission route or unmasking the true identity of those communicating. *Appendix 17 at 3:19- 4:10.*

The name "Ryan Pick" is derived from evidence obtained without a warrant. The motion to suppress evidence should be granted. *See* Va. Code § 19.2-65 and 18 U.S.C. § 2515.

Third Issue - The Court erred because the alleged victim, "Lilly," could not be a minor.

"Lilly is not a real person, is imaginary." *See Appendix 17 at 9:15-16.* Imaginary people don't exist, they do not live, they do not age, and therefore they cannot be under age. If she could age, this still presents a problem. One of the photos of "Lilly" provided as evidence (R. at 646)

was taken on July 7, 2008. This would make "Lilly" 23-years-old in 2018 when the alleged crime occurred. "Lilly" could not be a minor. The charges against Ryan Pick are for crimes against minors. Therefore, the charges against Ryan Pick should be dropped.

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.

ECPA statutes afford five general categories of privacy. All five are improperly handled in this case.

1. **Content (**Va. Code § 19.2-62 and 18 U.S.C. § 2511)

   A letter is equivalent to content: the body of a message including subject line and attachments.

2. **Meta-Data** and **Transactional Records** (18 U.S.C. § 2703(c))

   Envelopes are equivalent to meta-data. Addressees are equivalent to phone numbers or account names. Cancellation markings are equivalent to conversation start/stop times. Package weight is equivalent to megabytes transmitted. Phone records of who called whom are equivalent to IP address records of files downloaded.

3. **Routing and Geo-location** (Va. Code § 19.2-70(1-3), 18 U.S.C. § 3121, and 18 U.S.C. § 2703(c))

   P.O. box ownership is equivalent to online account ownership. Locating mail in transit is equivalent to identifying IP addresses or cell towers used for transmission.

4. **Stored Communications** (18 U.S.C. § 2701)

   Packages awaiting pickup at the post office are equivalent to emails or files awaiting download. After 180 days, it is "abandoned."

   Police ordering a post office to detain mail for police inspection is equivalent to police ordering a service provider to preserve electronic communication records and content.

5. **Subscriber Information** (18 U.S.C. § 2703(c))

   Requires a proper warrant.

Pick had a reasonable expectation of privacy. *See Appendix 3 at 76.* He was in his private home using his cell phone. His phone was protected with "electronic locks" in the form of a passcode or a username and password. He had a password-protected router in the communication path adding to his assumption of privacy. No warrants were obtained to unmask the identity of the anonymous Omegle user.

5.1 One Party Consent to Intercept and Record Private Communications

Payne claimed to be the "one party" who consented to interception and recording. Material facts in Pick's case present two concerns:

1. Payne created the imaginary person "Lilly" by combining characteristics of two different persons (two birth certificates): a female was the visual image and Payne typed the script. *See Appendix 17 at 9:13-15, 10:6-23.* This combination violates the legal definition of "person" as set forth in "We, the People…" and Article IV of the Constitution. A "person" is one human capable of having rights, not a composite of two humans formed to give the illusion of one human. A "person" has one birth certificate. 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).

2. Payne impersonated the person pictured, violating the "such person is a party to the conversation" clause. *See* Va. Code § 19.2-62(B)(2).

Lilly" was not only conjured out of the blue, she was also procured as if she was a person with rights for the sole purpose of intercepting communications and inducing people to commit a crime. "Lilly" by herself has no birth certificate.

Ms. Williams argued that distinguishing "between a real person and a fake person, the law really does not support this." *Appendix 17 at 11:10-12.* However, Black's Law Dictionary, 9th 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," *see 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.

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." Payne 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 female 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." See* Va. Code § 19.2-

62 (B)(2). Since ECPA applies equally to electronic communications, one cannot even auto-forward someone else's emails to an unintended recipient. *See U.S. v. Szymuszkiewicz***.**

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 name. *See U.S. v. Campagnuolo*, 556 F.2d 1209 (5th Cir. 1977). In Pick's case, no warrant was issued prior to obtaining his communications. No search was being executed at Pick's home. Payne did not answer Pick's phone. Payne initiated conversations on Omegle. Payne did not use his true name.

So, was the female depicted in the photo party to the conversations? She could not be because she did not participate in any communication. Was Payne impersonating the female in the photo? If so, "such person" in the photo was **not** party to the conversation. Or did Payne

manufacture an imaginary person? If so, cobbling together a composite profile consisting of texting by Payne and the visual image of the female does not meet the legal definition of "a person." In all ways, Det. Payne acted contrary to law.

A. Can officers Control Imaginary People?

Can an officer lawfully manipulate an imaginary person online to obtain private electronic, oral, or wire communications with an unwitting party under Va. Code § 19.2-62(B)(2) or Va. Code § 18.2-374.3? 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 birth certificate, 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. Imaginary people and cartoons do not comprehend friendship or faithfulness.

Payne testified that Lilly was a "geomorph," a creature where "the face was selected from one child, the eyes from another, the body from another so that no one child was actually used." *See Appendix 19 at 12 (101:6-17).* In other words, Lilly was a realistic **cartoon** created on a computer. The U.S. Supreme Court ruled that statutes can only be applied to images of "real" children, not computer-generated children. The provision that an image "is, or appears to be, of a minor" were ruled overbroad and may not even indicate exploitation of real children. See *Ashcroft v. Free Speech Coalition,* 122 S. Ct. 1389 (2002).

Cartoons have no standing to intercept or record conversations. The <u>intended recipient</u> of "Ryan's" communications was a cartoon animated by Payne. "Intended recipient" is clearly discussed in Va. Code § 19.2-62(C). Payne was not an agent of Lilly; he was not employed by

Lilly; he was not acting by Lilly's direction. Lilly was a creature of Payne, deployed as a deception to be the intended recipient of these messages.

There is a difference between being a participant in a conversation and lawfully being a person party to a conversation. Robo callers may be imaginary people who participate in conversations. A computer manipulates the Robo caller's 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.

Technology exists to manufacture the illusion of a human online – consider computer games. Computers combine visual images, voice, and dialog 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."

The Sixth Amendment guarantees that a defendant has a 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?

B. 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? Or 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 because your friend is not betraying you. 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 and 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 Payne was asked to send a picture of himself, he did not dress up in a disguise and send a photo of himself as "Lilly." Using a photo or being visibly present are two ways of establishing identification. Instead, Payne transmitted a photo of a female, not otherwise involved in this case. *See Appendix 19 at 11 (100:11-21).* A photo is a "means of identification" showing unique physical representation of a person, *see* 18 U.S.C. § 1028(a)(7), § 1028(d)(7)(B), and Va.

Code § 18.2-186.3(C). Payne created the character of the 14-year-old "Lilly" and assigned Lilly's personality to the female pictured, not to himself. In this way, he effectively thwarted the authenticity of identification a photo might provide. The female pictured was not party to any communication. Replies, intended for the female pictured, were instead intercepted by Payne and used to further the conversation. In *Grafmuller v. Commonwealth*, 290 Va. 525 (2015), one female officer projects 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 Pick's case, Payne and the female pictured are projecting the same persona "Lilly." Yet, "persona" means the social façade <u>one</u> person projects in public, <u>not two</u>. Payne <u>impersonated</u> the female pictured. The one and only flesh-and-blood "person" and true party to the conversation was "Ryan," and he did not authorize any interception or recording. There is **<u>no</u>** "color of law" exception in Va. Code § 19.2-62.

Court held that there is no requirement to prove communications involved 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 per Va. Code § 18.2-370 and § 18.2-374.3. However, *Deitz* failed to argue that § 19.2-62 precludes anyone from impersonation online to intercept communications, even law enforcement, and even with parental permission. *See Appendix 10 at 26.*

The conversations with "Ryan" were disclosed to the Court and used as the basis for charges brought against him. *See* Va. Code § 19.2-65. However, using or disclosing the content

of communications obtained via an unauthorized intercept is prohibited. *See* Va. Code § 19.2-62(A)(3) and § 19.2-62(A)(4).

C. Identity Theft

Through identity theft police investigative techniques violate the 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). A photo shows a person's unique physical representation and is a "means of identification." Payne's physical attributes do not match Lilly's. Payne procured the "means of identification" of someone else solely to intercept electronic communications with "Ryan." *See* Va. Code § 18.2-186.3(C) and § 19.2-62(A)(1). Payne had no legal authority to intercept "Ryan's" communications because Payne was NOT the intended recipient of those communications – the female identified by the photo was the intended recipient.

In *U.S. v. George*, No. 19-4125 (4th Cir. 2020), the court held that 18 U.S.C. § 1028A(a)(1) defined "person" to include those living and dead, NOT imaginary people. The female pictured appears to be a living person. Payne's use of someone else's photo as his own identification in order to intercept communications meets the definition of identity theft.

A "WANTED" poster consists of a photo for identification and either the given name, e.g. John Dillenger, or the persona's name, e.g. Billy the Kid. In the hypothetical WANTED poster (below left) Lilly is shown wearing her "ALLSTAR 07" T-shirt. In this example for whom would the police be searching? The "Lilly" girl in the dated photo? Det. Troy Payne? Or Yesli Vega (the likely adult version of the girl in the photo)? Interestingly, in Vega's public campaign speeches for Prince William County Supervisor she claimed her law enforcement career began in the Richmond area around 2008.

WANTED

"Lilly"

(R. at 647)

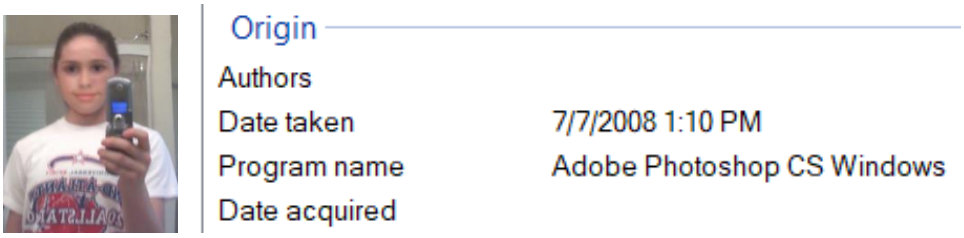
Yesli Vega (2018)

(Campaign website photo)

What police refer to as simple investigative techniques, however, cross the line into theft of identity. Payne clearly procured the "means of identification" of someone else solely to intercept electronic communications with "Ryan."

D. Abuse of Technology Can Lead to Entrapment

Defense attorney Jones argued that "Lilly" was the persona of a 13-year-old. *See Appendix 17 at 5:23-6:2.* He was corrected by Williams who replied, "Lilly is not a real person, is imaginary." *See Appendix 17 at 9:15-16.* Mr. Jones conceded her point. Imaginary people don't exist. They do not live lives. They have no birth certificate. Therefore, how can an imaginary person 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. Black's Law Dictionary, 2nd Ed.



The jurors were shown the photo above of 13-year-old "Lilly" taken July 7, 2008. *See* (R. at 646) *and Appendix 19 at 12-15 (101:23-104:5).* The "ALLSTAR 07" T-shirt also denotes the year 2007. Who would assume that Lilly, wearing a 2007 T-shirt in a picture taken in 2008, would not be an adult by 2018? What "geomorph" editing capability existed in 2008? *See Appendix 19 at 12 (101:6-17).* Similarly, it is all the more ridiculous when one considers "Heather Boon," the longtime persona used by Det. Wells. She was 13-years-old in 2001 *(see Hix v. Commonwealth,* 042717 (Va. 2005)), but only age 14 by 2016. *See Commonwealth v. Hawthorne* (Stafford County, 2016), *Appendix 11 at 1.* The Omegle conversation did not occur with a minor, it occurred with an adult. The charges against Ryan Pick are for crimes against minors. The persona, "Lilly," was not a minor.

The Courts have long recognized that police may use subterfuge in legitimate investigations. *See Appendix 17 at 19:22-23*. But in order to lawfully participate in a conversation and intercept the communications, police must be capable of holding the conversation while being "visibly present." This criterion to safeguard Fourth Amendment protections was not met. *Appendix 1 at 15, sec. 3.5(c)*.

Moreover, what probable cause to investigate a crime exists after a stranger says, "hello?" "Ryan" (like others) began conversing anonymously with someone he thought to be a real, adult person. Payne "created this imaginary person solely for the purpose of obtaining, or intercepting, the electronic communications of a target." (R. 70¶8). Payne was "manufacturing and sending out textual messages as if they came from Lilly" in order to induce an unwitting target to violate the law. (R. 70¶7). What predisposition does an officer have to use an imaginary persona and initiate a private online conversation with a random stranger? *See Appendix 17 at 10:4-6.* Payne was effectively a 3rd party controlling and monitoring a non-person, beginning at "hello."

Va. Code § 18.2-374.3(C)(D) requires proof of "lascivious intent." Yet the idea of the crime and detailed instructions for how to commit it were provided by Payne. *See Appendix 19:*

1. Payne first requested a risqué visual image:
   "Wish I could watch," at *20 (109:8-9)*

2. Payne repeated this request when a visual was not provided:
   "wish I could see" *at 25 (114:21)*

3. Payne recommends using Dropbox to transmit visual images:
   "I have a drop box," *at 20 (109:12)*

4. Payne directs "Stranger" to make a Dropbox and deposit pictures in it:
   "you should make a dropbox and send me a pic of you" *at 22 (111:11-12)*

5. Payne first requests a meeting:
   "would you ever want to meet me?" *at 23 (112:10-11)*

6. Payne first requested a risqué video:
   "you could db a video too. Neck down or something." *at 26 (115:3-4)*

7. Payne repeats the request for a risqué visual image a third time:
   "I want to see you" *at 26 (115:5)*

8. Payne gives "Stranger" detailed instructions when "Stranger" doesn't know how to commit the crime:
   "How do I send you the link?" *at 26 (115:12-13)*
   Payne replied with detailed instructions on how to commit the crime:
   "you put the pic in your db. Right click the pick and copy the link. Then paste it here." *at 26 (115:13-14)*

Ryan Pick was nevertheless found guilty of sending a lewd video. *See Appendix 3 at 84¶4.*

In a related case, *Jacobson v. United States*, 503 U.S. 540, 548 (1992), officers sent unsolicited child pornography catalogs through the mail to the defendant, who eventually placed an order. A search of Jacobson's home found only pornography sent by the Government. The Court ruled "Government agents may not originate a criminal design, implant in an innocent person's mind the disposition to commit a criminal act, and then induce commission of the crime so that the Government may prosecute."

Payne used trickery, persuasion, and fraud during his "investigation." By abusing technology Payne could hide behind a photo posted online and pretend to be a young girl. He used the girl to manufacture a criminal. If this isn't entrapment, what is?

E. 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.

F. 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 Va. Code § 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 Va. Code § 18.2-374.3 but does not in § 19.2-62. Payne cannot be 'such person' and 'party to the conversation,' pursuant to § 19.2-62, while simultaneously claiming he is Lilly shown in the picture, pursuant to § 18.2-374.3. If the court concludes that Payne impermissibly intercepted communications (pursuant to § 19.2-62 *seq*.) and Pick's rights were violated, then the charges against Pick cannot stand.

G. Using a Phones and Computers as Interception Devices

Judge Harris asked, "So if I'm using one device to communicate with another device, did the General Assembly intend that the device itself, the one that I am communicating to, is intercepting the communication, and I don't think so." *See Appendix 17 at 17:10-14.* Judge Harris correctly understood one type of interception, but disregarded the fuller meaning of interception contained in the statute. He incorrectly ruled that simply being a participant in a conversation also implies being a lawful party to the conversation. Anytime a conversation is recorded by a participant who is <u>not</u> lawfully "such person" party to the conversation, the device is being used as an interception device. *See* Va. Code § 19.2-62(B)(2).

In online sting operations, undercover officers troll on social media sites without probable cause or warrants. *See Appendix 17 at 10:4-9.* Payne intentionally used Dropbox deceptively, falsely identifying "that he's a female and he's thirteen years old," and that "Lily" sent the images over Dropbox. *See Appendix 17 at 6:15-22 and 10:21-23. See also Appendix 19 at 20 (109:11-15).* Many such sites have user agreements that expressly prohibit this practice. Dropbox prohibits *(See Dropbox Terms of Service (April 16, 2019), Appendix 16 at 9):*

- "deceptive or false source-identifying information."
- "sharing material that's fraudulent … or misleading"
- "violate the privacy or infringe the rights of others."

A user is defined as "any person duly authorized by the provider to engage such use." Va. Code § 19.2-61 and 18 U.S.C. § 2510 (13)(b). A Virginia detective is not duly authorized by the provider (Dropbox) when he violates their User Agreement; therefore, he is not a lawful user of the application. Since the application becomes a component of the computer or phone, one must use it in accordance with user agreements. Otherwise, the device and components were not being used in "ordinary course of business," but as an interception device.

H. Wiretapping without Authorization

Electronic communication content receives the highest degree of privacy protection under law. Payne did not communicate with Pick on Snapchat. Yet, Williams obtained Pick's private Snapchat conversations with five other people and disclosed it to the Court. (R. at 134-135). Williams included portions of three of these conversations in her motion *in limine* to admit them as evidence. (R. at 101-103). *See* Va. Code § 19.2-62(A)(3,4) and 18 U.S.C. § 2511 (1)(c,d).

Snapchat does not preserve content. "We don't stockpile your private messages." *See "Our Privacy Principles, Privacy Policy, Snapchat.com"* (October 1, 2018), *Appendix 15 at 1*. Communications temporarily stored while in transit or awaiting retrieval are covered by the Stored Communication Law (18 U.S.C. § 2701), though Snapchat stores nothing. How then was Pick's content obtained? Snapchat's privacy policy states:

> *Snapchat servers are designed to automatically delete messages sent in one-on-one Chat after both Snapchatters have opened and left the Chat (Appendix 15 at 2 ¶2).*
>
> Snapchat servers are designed to automatically delete all unopened Chats after 30 days *(Appendix 15 at 2 ¶3).*

Pick and those with whom he was communicating viewed all Snaps and opened all messages. His messages could not exist 180 days later because Snapchat deletes both read and

unread messages at the 30-day mark *(Appendix 15 at 2 ¶3).* Messages left by the customer, but stored "180 days or fewer have the highest level of protection under ECPA." *See Appendix 3 at 80¶4 and 81¶2.* Communications stored more than 180 days, however, are considered by the law to be abandoned, requiring only a written statement certifying that the information is relevant to an investigation. *See* 18 U.S.C. § 2703(a). Because all Pick's messages were downloaded and read, they were not stored by the customer, and they were not abandoned "stored communications." Virginia AG's report affirms no intercept authorization was granted. *See Appendix 4 at 13-16.* Clearly, a request was communicated to Snapchat asking it to store Pick's messages. Why else would Snapchat, favored for its instantaneous deletion of texts, ignore its own policy to save these messages so they could later be retrieved by Williams after the 180-day point? Snapchat could only intercept and "stockpile" Pick's communications under one of two conditions:

1. The Virginia AG's office authorized the interception. (*Appendix 15 at 9¶3)* or

2. Snapchat didn't follow its own policies-in-practice, instead expending tremendous resources on electronic storage to hold all their users' chats.

Va. Code § 19.2-68 *and* 18 U.S.C. § 2516 outline procedures for law enforcement to order interception and storage of communications. *See U.S. v. Giordano*, 469 F.2d 522 (4th Cir. 1972) for proper procedure. Moreover, the charges against Pick do not allow for an authorization under Va. Code § 19.2-66(A). *See also Morton v. Commonwealth*, 315 S.E.2d 224 (1984). Significantly, Payne is not employed by Virginia State Police, the only entity which may conduct a lawful interception, and then only under certain circumstances. *See* Va. Code § 19.2-68(C)(4). Virginia

AG *Annual Report on Number of Applications for Intercept Orders* (per Va. Code § 19.2-70) listed no authorization requests to intercept for solicitation 2010-present. *See Appendix 4 at 1-16.* Querying a selector (phone number, or here, a Snapchat account name) is a potential violation of law even when it returns no content data. *See* NSA / Central Security Service *IG Report of Investigation (9 January 2014), Appendix 8 at 2-4.*

Service providers like Snapchat may perform random monitoring of service but cannot lawfully target any particular user for monitoring or collection. *See* Va. Code § 19.2-62(B)(1) and 18 U.S.C. § 2511 (3)(b)(iv). Searching selectors like "stonynots" requires approval of the Attorney General or Deputy AG. *See* United States Signal Intelligence Directive (USSID SP0018) *Legal Compliance and U.S. Persons Minimization Procedures, Appendix 5 at 6 sec. 4.1(b) and 13 sec. 5.4.*

Apparently, a search warrant (dated April 22, 2019) was eventually sent to Snapchat. Pick claims he was not served with this search warrant and was unaware of its existence until referenced in Commonwealth's motion (R. at 147), argued on Aug 16, 2019. *See Appendix 18 at 02-09.* Where is the search warrant?

Furthermore, why was this search warrant implemented 8 months after Pick's arrest? Could it be that 8 months is longer than 180 days, making it so Pick's communications could be categorized as "abandoned" and obtainable with just a search warrant? This would effectively bypass law requiring any Court authorization to intercept communications. Whenever "active" stored communications transition to "abandoned" status at the 180-day point, it is dependent upon the **customer's** failure to retrieve or delete the communication. **It does NOT depend on Law Enforcement ordering the interception and storage of communications** that would otherwise be deleted.

Snapchat's response to this search warrant yielded content, however. (R. at 147). Yet, how could a search recover nine-month-old content when it was not stored in the first place? Snap Inc., *Law Enforcement Guide (Sept. 21, 2018) at 11* states that Law Enforcement may obtain content by submitting a Preservation Request. Since content was obtained, it is fair to assume a Preservation Request was sent. (R. at 149-150). Where is the Preservation Request, pursuant to 18 U.S.C. § 2704? Who authorized it? Where is Pick's official notification informing him that his account was being preserved, pursuant to § 2704(a)(2) so he might challenge this action?

Initially, an administrative subpoena was sent to Snapchat requesting subscriber information about Pick's "stonynots" account for the 90 days prior to July 12, 2018. *See Appendix 13 at 10*¶*5.* This returned basic subscriber information. *See Appendix 14 at 9.*

Response to the search warrant reveals a similar absence of conversations before July 12th. Yet, on July 16th, content was clearly intercepted. (R. at 149-150). Who ordered interception and preservation of communications within Pick's Snapchat account? Where is the Court order, pursuant to 18 U.S.C. § 2703(f)(1)?

Assistant A.G. Williams, during her prosecution, surely understood the content of Pick's "stonynots" communications were obtained without proper authorization. Warrantless "wiretaps" violate Va. Code § 19.2-68 *and* 18 U.S.C. § 2516. *See Mitchell v. Forsyth*, 472 U.S. 511 (1985).

I. 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 10 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.

J. Electronic Warfare against U.S. Citizens

Judge Harris asked, "How many – how much deception is the line? Where, you know, is the officer saying that he's female, is that enough? Is the officer saying that he's female and thirteen, is that enough?" *See Appendix 17 at 19:22-20:1.* Sting operations where officers post pictures of teens and impersonate them meet the federal government's technical definition of electronic warfare against U.S. persons. Joint Publication 3-13.1 *Electronic Warfare (2012) Appendix 7,* defines "the line;" deception against U.S. persons crosses "the line."

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 a communication 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 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, <u>including wireless telephone</u>. (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, Payne sent communications on Omegle, masked to look like it came from a trusted source, "Lilly." Payne transmitted a deceptive message with a picture of someone else (using an EMS signal) to the suspects electronic device (launching an electronic warfare attack). The suspect reacted to this communication in a manner detrimental to him: Pick

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

5.2 Pen Register / Tap and Trace Devices

Typically, a user's true name and address is not attached to email addresses or to usernames of computer applications. Yet, the name and address of Pick are listed in Court documents. How was this information obtained? It appears that police use commonly available products as *de facto* pen register / tap and trace devices to obtain one's name and address without a lawful warrant.

Va. Code § 19.2-61 *et seq.* and 18 U.S.C. § 3121 *et seq.* not only afford Fourth Amendment privacy protections to individuals when they transmit information, but the law also protects the ***ownership*** of the recipient account and safeguards ***transmission routes*** used, obscuring their ***geographic location***. *See Appendix 3 at 78.* Use of a device or process to obtain such information requires a pen register / tap and trace device warrant. Pen registers track where messages go. Tap and trace devices determine messages' origin.

U.S. Supreme Court has ruled that tracing a phone number dialed to determine the owner requires a pen register warrant. *See Smith v. Maryland,* 442 US 735 (1979). Identifying the owner of an email address also requires a warrant. *See McVeigh v. Cohen,* 983 F. Supp. 215 (D.D.C. 1998). U.S. District Judge Stanley Sporkin wrote:

> [I]*t is elementary that information obtained improperly can be suppressed where an individual's rights have been violated. In these days of "big brother," where through technology and otherwise the privacy interests of individuals from all walks of life are being ignored or marginalized, it is imperative that statutes explicitly protecting these rights be strictly observed.*
>
> *That the Plaintiff may have made incriminating statements at the subsequent administrative hearing does not bootstrap the Navy out of its legal dilemma of not only violating its own policy, but also a federal statute.*

The U.S. Supreme Court also recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements, so a cell phone's geographic location is protected. A cell phone's location can be obtained by mapping cell towers the phone connects with and noting time the user made calls. Acquiring such information requires a warrant. *See Carpenter v. United States*, No. 16-402, 585 U.S. _ (2018). Pick's cell phone was the alleged device used to communicate on Omegle, where a video was supposedly created and transmitted. Somehow, police on July 10th determined Pick's cell phone was geographically located in "Woodbridge." Obtaining an IP address or geographic location from the transmission (vs. from subscriber info) requires a warrant. *See* Va. Code § 19.2-70 (1-3). "IP addresses the subscriber visited" are similar to the IP address of one's home router and must be obtained via warrant, not subpoena. *See Appendix 3 at 79 bottom - 80 top.* This warrant was never obtained.

The federal government trains personnel to mask (minimize) any intercepted phone number or other identifier of a U.S. Person to protect one's privacy. *See Appendix 5 at 28-34.* Per DoD Directive, any communications between U.S. Persons, even incidentally collected must be destroyed. Other agencies of the federal government also follow these same practices.

Privacy considerations apply to IP addresses as well as phone numbers. An internet service provider assigns an IP Address to routers, commonly used in homes, allowing electronic devices to communicate over a network. Today, commercial tools protect privacy by intentionally generalizing information of their users. This means the geographic location (town name) of IP addresses is made vague to ensure there is no more than a 1 in 10,000 chance of accurately identifying a person by name, address, town, phone, etc.

A. Dropbox-Like Applications

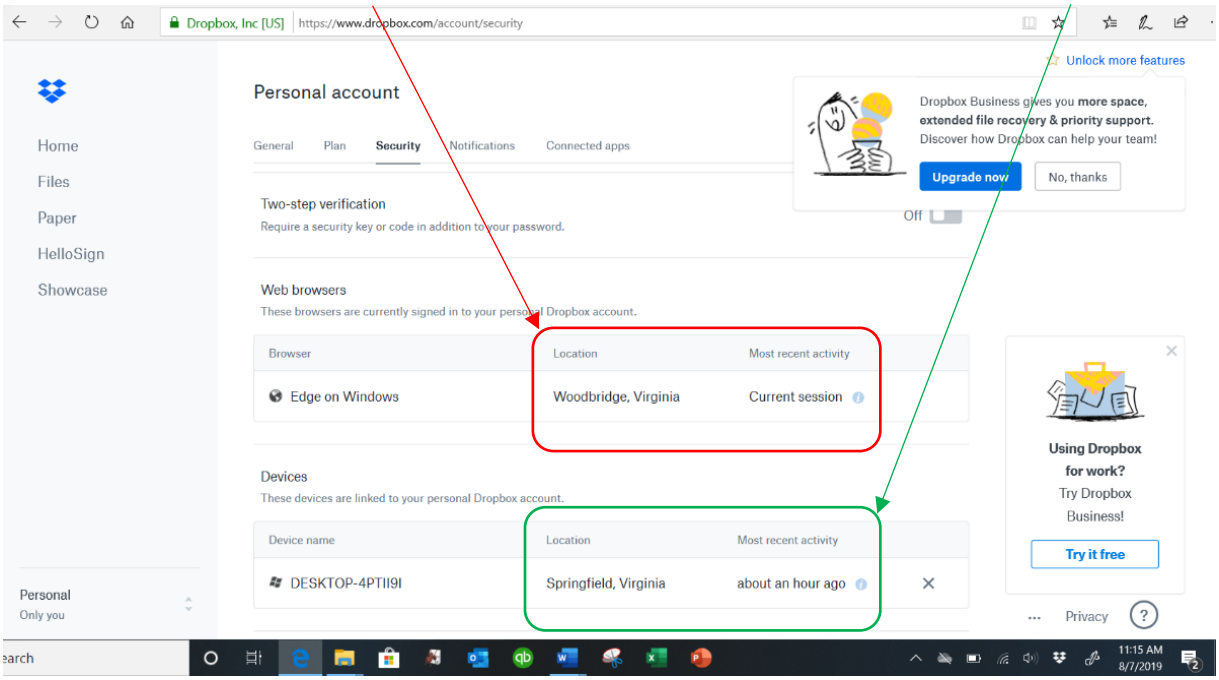
Online undercover operations are conducted on dating apps or in anonymous chat rooms. These sites deliberately mask the user's true name, town, and IP address to protect their customer's privacy as required by law. In order to thwart these privacy safeguards, police use Dropbox and similar apps as a "proactive undercover technique" in lieu of a standard pen register / tap and trace device (*see Appendix 3 at 51 bottom)*. They can then save time and circumvent having to obtain a warrant. A police officer sends a hyperlink containing a picture to a target. When the target clicks on the hyperlink, the target's identity is unmasked. This unmasking reveals private information such as the anonymous user's identity or geographic location in same way a pen register would, but without the trouble of a warrant. Police then obtain a subpoena for what they have already found. But people have a right to remain anonymous. *See U.S. v. McIntyre*, 582 F.2d 1221 (9th Cir. 1978) and *Talley v. California,* 362 U.S. 60 (1960).

Peer-to-peer file transfer products like Dropbox, Shareaza, or Ares provide easy file transmittal directly from one computer to another. These products collect ancillary information to perform common tasks, such as finding coffee shops in the user's geographic area. For example, financial institutions can log such information to track possible theft of electronic papers. If such theft was reported to police, officers could obtain a pen register warrant to identify the suspect. However, the method to collect ancillary information is what the police exploit.

Dropbox confers exclusive administrative rights to the user who creates a Dropbox for a set purpose. This one user gains the ability to view the IP address and approximate town name at the other end of a file transfer. No other user in the group can view this transactional data. Another technique is for a user to create a link from an IP address logger and send this link within an electronic communication. The effect unmasks the IP address of anyone who clicks the link.

These two techniques allow police to acquire transactional records and hidden transmission route information which can be used to identify and locate suspects, thereby skirting the law.

I tested this theory and drove to Woodbridge, VA. The WIFI in Starbucks showed I was located in Washington, D.C., 24-miles away. Two blocks away, the WIFI in Wegman's showed I was located in Woodbridge, population over 50,000. These WIFI providers intentionally generalized their geo-location as required by law to protect the privacy of their customers. The information below illustrates my use of Dropbox with the WIFI at Wegman's (see left red arrow: "Current session"). An hour earlier I was in Springfield and had used a different account to remove a file from the same Dropbox I created previously (see right green arrow: "about an hour ago").



Let's apply this explanation to the present case. On July 10th, "Stranger" chatted on an anonymous, private chat application called Omegle. *See Appendix 19 at 08 (97:14-18).* "Stranger" clicked on a Dropbox hyperlink provided by "Lilly" (Det. Payne) and saw an innocuous picture. *See Appendix 19 at 20 (109:11-16).* Merely viewing a picture in a Dropbox creates an electronic

pathway directly between the two computers because Dropbox is a type of peer-to-peer file transfer program. Payne was able to capture the underlying network transmission route and geo-locate the suspect viewing the picture. At this point, "Stranger" had not committed a crime. When provided an IP address, Shareaza-LE is theoretically accurate to the street. If so, it would allow an officer to geo-locate an anonymous Omegle user before continuing the conversation and before commission of a crime. *See* Shareaza User's Manual (online) (Feb. 2, 2014), *Appendix 9 at 31, entry 22:53.*

On July 10th, Payne claimed he searched using the term "Woodbridge" in Google (*see Appendix 13 at 10¶2*), pointing to Ryan Pick as the suspect. The word "Woodbridge," did not appear in the intercepted Omegle conversation Payne supplied to the Court. On July 17, Payne submitted an administrative subpoena (not a warrant) to Verizon Fios to identify the owner of this particular IP address. *See Appendix 13 at 10¶5.* The response was returned on July 18th indicating the town name "Woodbridge." *See Appendix 13 at 11¶1-2.* Therefore, "Woodbridge" could only have originated from an earlier source – the Dropbox used as a *de facto* pen register device on July 10th. I witnessed an *ex parte* conversation in the Courthouse hallway where Attorney Jones asked Williams where the search term "Woodbridge" originated. Later, Williams would not confirm that police used the search term "Woodbridge" to identify Ryan Pick and would only confirm terms "Ryan" and "music teacher" were used. *See Appendix 17 at 10:24-25.* Payne also refused to explain how he obtained the term "Woodbridge" on July 10th and how he connected it to Pick. *See Appendix 19 at 29 (118:1-12).* How could the term "Woodbridge" be used on July 10th, 8 days earlier, to determine the name of the suspect as "Ryan Pick" if Verizon had not yet revealed that information? The subpoenas appear to be an after-the-fact addition to create a veneer of following proper police procedure.

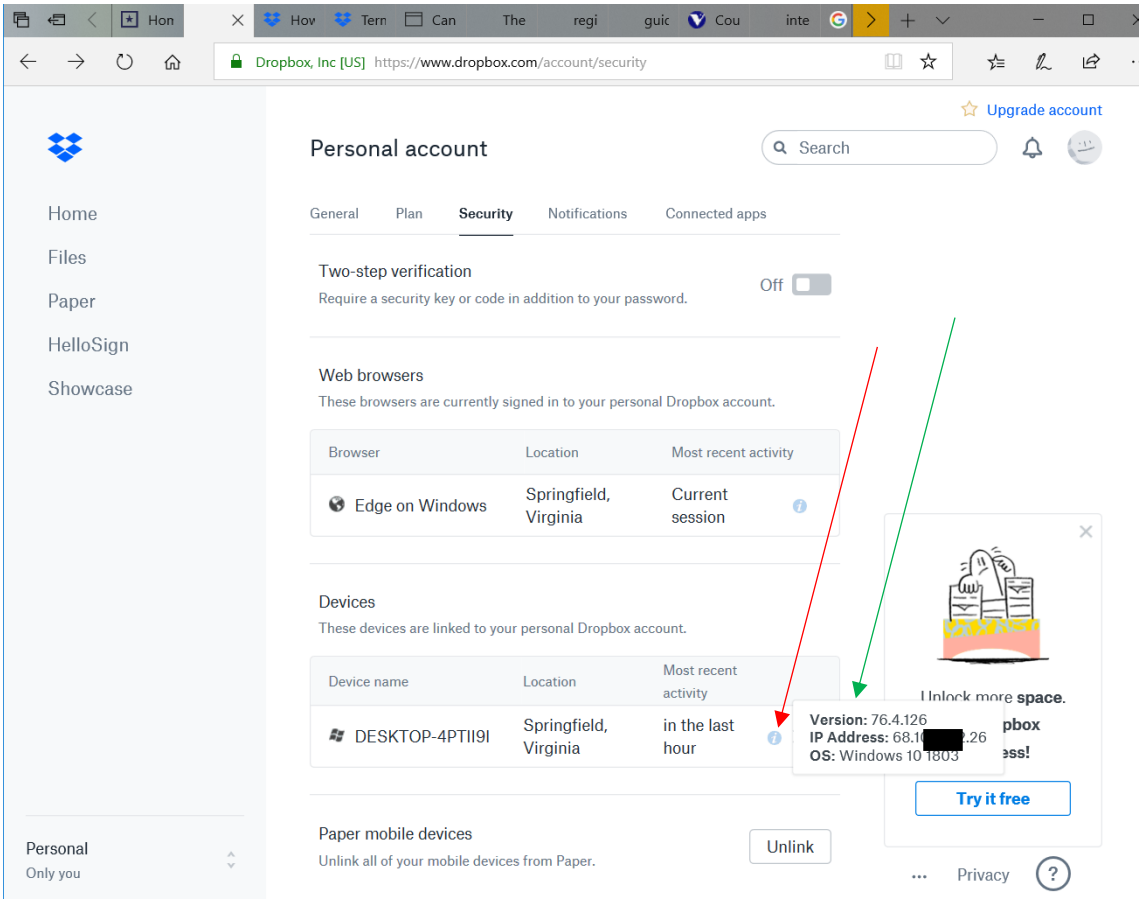
Google search terms "Ryan," "music teacher," and the Snapchat account "stonynots" were obtained without first securing a warrant to intercept communications. *See* Va. Code § 19.2-68. It is speculation to assume "Stranger's" true name was "Ryan" since the Omegle application does not verify identities. No warrant was ever issued to obtain the IP address from Snapchat account "stonynots," only an administrative subpoena dated Jul 11th. *See Appendix 13 at 10, ¶5.*

Police secured no warrant to use *Maxmind.com* on the IP address in order to obtain the service provider Verizon or generalized town name "Woodbridge." *See Appendix 13 at 11¶1.* Maxmind's latest estimate on geo-location precision states they are "80% accurate on a state level" and "68% accurate for cities … within a 50 km radius." *See Maxmind Geo-location Accuracy, Maxmind.com (August 17, 2019), Appendix 20 at 1-2.*

I have never encountered a website so infected with computer viruses, malware, etc. as *Maxmind.com*. Although I only looked at its webpages and never used the tool, my computer security program constantly sounded alarms, stopped unrequested programs from running on my computer, and prevented me from accessing Maxmind's main page. *See Appendix 20 at 2.* I could only jump directly to a subpage that fortunately held the statistics I needed. Yet, we are to believe that this is the website Payne used to obtain "Verizon" which led to "Woodbridge." *See Appendix 13 at 10-11.*

Payne's story makes more sense if we understand Dropbox capabilities. Dropbox can easily be used to identify the IP address as well as geolocate the town, whereas Maxmind is problematic. The graphic below demonstrates one must be skilled to use the IP address features of Dropbox. Clicking on the lower case "I" in the bubble (left red arrow), allows the Dropbox owner to see the IP address (right green arrow) of another person pulling a picture out of the Dropbox (the actual IP address is redacted for privacy). Which tool did they actually use?

Remember, Shareaza-LE is supposedly accurate to the street when provided the IP address. *See Appendix 9 at 31, entry 22:53.*



Courts have upheld a person's right to remain anonymous even when online in a public blog and posting a simple textbook. *See Signature Mgmt. Team, LLC v. Doe*, 323 F. Supp. 3d 954 (E.D. Mich. 2018). Law enforcement must obtain a warrant to electronically track one's geographic location**.** *See U.S. v. Jones*, 565 U.S. 400 (2012). "Special authorization is required to obtain information protected by the Fourth Amendment." *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 6.* "If the technique or method being considered seems to require specialized

tradecraft or skills, or is typically used in clandestine ways, then that is an indicator that legal counsel should be consulted" and "… instructions on a blog for how to penetrate a bank's online security, the bank's data does not become lawfully available as a result." *See Appendix 6 at 7.*

Simply put, either police do not understand what they are doing requires a high-level scrutiny that a simple subpoena cannot offer, or they don't care. One's privacy is at stake.

B. Use of Network Investigative Technique (NIT)

If someone wants to hide their IP address when doing illegal activity such as downloading pornography, they use systems such as "Tor Project" to mask their electronic trail. Police use a NIT to track down this hidden IP address. A NIT operates as a pen register device attached to a file. The NIT can be attached to a file containing pornography and "hitchhikes" along. It invades the host computer, forcing it to send to the FBI the computer's IP address, host name, and username. The FBI routinely uses this method, obtaining a warrant to attach NIT to files. The NIT lawfully and successfully told the FBI where the files went. *See U.S. v. Taylor,* No. 17-14915 (11th Cir. 2019).

5.3 Other Questions for the Court

A. Does an offense against an imaginary person require registering as a Sex Offender?

34 U.S.C. § 20911 categorizes the Sex Offender Registry into two types of offenses: violent and non-violent. This statute depends on a crime being committed against a "minor," who is "an individual who has not attained the age of 18 years." Imaginary people don't attain age. The imaginary person, "Lilly," cannot be underage, nor can she grow older. One photo of the imaginary 13-year-old "Lilly" showed it was created July 7, 2008. Was "Lilly" age 13, or based on the photo's creation date, age 23?

This definition of the Sex Offender Registry does not have any category for crimes against an imaginary person, cartoon, or an officer impersonating someone else. The key phrase "has reason to believe" is a minor does not appear in this statute. *Hix v. Commonwealth* suggests that a suspect may be guilty of an offense based solely on interpreting the statutory language "has reason to believe" the victim was a real child, pursuant to 18.2-374.3. This decision failed to defer to the older, federal-based statute of Va. Code § 19.2-62 as well as 34 U.S.C. § 20911, both of which have no category for crimes against imaginary people, cartoons, or people impersonating someone else. The interpretation of *Hix v. Commonwealth* is overbroad because it includes a category of crime that doesn't really exist: sending a text message to an imaginary person or cartoon.

A typical conversation consists of one person communicating their thoughts to another person some distance away. The interpretation of *Hix* considered only the defendant's end of the communication in terms of his intent. *Hix* fails to take into account the statutory requirement that a person at the other end of the communication can neither be an impersonator nor an imaginary person. Both Va. Code § 19.2-62 and 34 U.S.C. § 20911 requires both ends of the communication to be actual human beings capable of having rights, not imaginary people.

The statutory intent was to protect actual minors. The statutory language repeatedly speaks of offenses against or involving an actually "minor." Here, there is no real victim. This is not an offense recognized by the sex offender registry statute. Therefore, the Court should rule that one cannot be compelled to register as a sex offender (violent or non-violent) when no actual minor is involved.

B. Is the Eighth Amendment violated?

A violation of Va. Code § 18.2-374.3 is considered a violent sexual offense on par with rape. How is sending a risqué text message to an imaginary person a violent act? "Violent" means "assailing the person with a great deal of force." Black's Law Dictionary, 2nd ed. One cannot assail an imaginary person, let alone assail one with a great deal of force.

Violations of Va. Code § 18.2-374.3 also require registration on Virginia's Sex Offender Registry, yet there is no such registry for other heinous crimes. Using a branding iron to permanently scar criminals with a scarlet letter or force someone to wear an armband or patch as public stigmata has been deemed cruel and unusual punishment. Excessive punishments have been overturned. *See Timbs v. Indiana* 139 S.Ct. 682 (2019). This registry also discriminates against innocent people who provide offenders lodging or employment. It brands any locations where those on the registry work and live, as well as people who provide them work or shelter - like my husband and me.

Upon Mr. Hawthorne's release from jail, he registered as a sex offender as required. He was unable to live with his family until certain Court requirements were met, so he lived with us for 2½ months. He returned to his home, but my home continues to appear in sex-offender mapping programs. My home, my husband, and myself are forever branded, yet we did nothing more than show Christian compassion. We are members of a golf club and had invited Mr. Hawthorne and his family to watch fireworks, July 2019. The mere sight of our guest, Mr. Hawthorne, generated complaints from others at the clubhouse. Management reprimanded my husband and instructed him to never bring Mr. Hawthorne on the premises again. Pick and others like him will have to register and will share a similar fate.

In what way does a rapist pose the same level of public safety risk as this violation? *See* Va. Code § 9.1-902(B)(1). Shouldn't drug dealers, murderers, armed robbers, or kidnappers also have a Registry? These other heinous crimes have no "sex" stigma associated with them. No law requires third-party sex-offender notification systems to maintain accurate, up-to-date data. The length of time on Virginia's sex-offender registry is now 25 years, near permanent discrimination in employment, housing, travel, and custody of their children.

The Eighth Amendment also prohibits "sentences that are disproportionate to the crime committed." See *Solem v. Helm*, 463 U.S. 277 (1983). Excessive punishment for other crimes has been overturned by the Supreme Court. *See Austin v. U.S,* 509 U.S. 602 (1993).

In *U.S v. Bajakajian*, 524 U.S. 321, 334-40, (1998), the U.S. Supreme Court considered four factors when determining if the punishment is appropriate to the offense:

1. Nature and extent of illegal activity – there was no probable cause a crime was being committed. There was no real victim.
2. Does the defendant fit into the class of persons for whom the statute was principally designed – this is a crime against an imaginary person; not a crime against a person, the original intent of the statute.
3. Considering the maximal penalties that a court could have imposed – mandatory 5 years in prison with 5-30 years possible.
4. Harm caused by the offense – the imaginary person was not harmed. The detective controlling the imaginary person was not harmed. No person was harmed in this crime. No property was damaged through this crime.

Being labeled a "violent sex offender," serving 7 years in prison, then serving 25 years on the sex offender registry is excessive for any offense against an imaginary person. This punishment for sending communications to a cartoon violates the Eight Amendment.

C. Does sending a risqué message justify denying bond?

Decisions to award or deny bond are based on "an unreasonable danger to himself or the public." Va. Code § 19.2-120. What unreasonable danger is there if the "minor" is an imaginary person? We have different penalties for various levels of murder, from involuntary manslaughter to premeditated murder. Why is rape considered on par with sending a text message to an imaginary person? Might the offender push the buttons on his phone more violently? How does that fact justify denying bond? Clearly there is no danger to the public here. There is only a reactionary standard – no bond for sex offenses, regardless of facts.

Most men charged with violating Va. Code § 18.2-374.3 are denied bond. *See* Va. Code § 19.2-120(A)(2) *and* § 19.2-120(B)(8). Doesn't this violate one's Eighth Amendment Rights?

5.4 Authorizations to Intercept

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

intercept and monitor under carefully control circumstances and with prior 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 (like Ohio) and Federal statutes expressly state the manner in which law enforcement officers can be a party to a 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 by contrast, and does not exempt law enforcement acting under the color of state law and does not provide that they are a party to a communication. Neither does the Federal or Virginia law grant authorization to impersonate anyone else during 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.

6. Conclusion

When our forefathers penned the words "We, the People," they did not have in mind imaginary people, cartoons, or consider impersonators to mean "the People." When they penned "The right of the people to be secure in their persons, houses, papers, …" they meant actual flesh-and-blood "people." "Papers" include electronic papers. They saw no need to provide exceptions permitting such methods or using gadgets like Shareaza-LE because "the ends [could not] justify the means."

"Courts are not permitted to rewrite statutes," Constitution, or the Fourth Amendment. *Last v. Virginia State Board of Medicine*.

If the Court disagrees with my arguments, then police (with no color of law exception or warrant):

- Can combine multiple images (geomorph) that speak and text according to what an officer types at a keyboard. The person depicted in the image may be real, partially-real, or a cartoon. Their likeness and manufactured voice could be used to intercept communications for they would be lawful parties to any communication.
- Can manipulate imaginary people to induce someone into committing a crime.
- No one can be secure in their person, house, or papers unless they self-quarantine from the digital world.

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, a right to remain anonymous, and a right to privacy of their geographic location free from unwarranted electronic tracking.
- Law enforcement must obtain a warrant to violate these basic Fourth Amendment principles upheld in Courts.
- Evidence obtained in violation of ECPA statutes and derived therefrom should be suppressed. The charges against Ryan Pick are for crimes against minors. "Lilly" was not a minor. Charges should be dismissed accordingly.

The Virginia Attorney General is charged with enforcing these laws, but took no action when I reported violations. *See Burkhardt Letters to Virginia AG, Appendix 12.* The public may have been convinced that sting operations using imaginary people are necessary before a real child is harmed. However, 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. Qualified immunity should not apply since these operations and resulting prosecutions violated federal and Virginia statutes from the outset.

Respectfully submitted,

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

Dated: March 17, 2020