IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

ASHLEY POPA, *individually and on behalf of all others similarly situated,* *Plaintiff,* v. HARRIET CARTER GIFTS, INC. *a Pennsylvania corporation* and NAVISTONE, INC. *a Delaware corporation,* *Defendants.*	Civil Action No. 2:19-cv-450 Hon. William S. Stickman IV

OPINION

WILLIAM S. STICKMAN IV, United States District Judge

Plaintiff, Ashley Popa ("Popa"), brought this class action on behalf of herself and all others similarly situated against Defendants, Harriet Carter Gifts, Inc. ("Harriet Carter") and Navistone, Inc. ("Navistone"), alleging that they violated the Pennsylvania Wiretapping and Electronic Surveillance Control Act of 1978 ("WESCA"), 18 Pa. C.S. §§ 5703–5728, by unlawfully intercepting her data while she shopped online. (ECF No. 38, ¶¶ 1–2). Defendants filed a Motion for Summary Judgment as to Count I (ECF No. 91).[1] For the reasons that follow, the Court will grant Defendants' motion and enter summary judgment in their favor.

I. BACKGROUND

In early 2018, Popa visited Harriet Carter's website, www.harrietcarter.com, where she provided her email address, searched for pet stairs, and added one or more items to her online cart

[1] This is the only count that remains in the case. The Court, on December 6, 2019, dismissed Popa's other count, which consisted of an allegation that Defendants committed tortious intrusion upon seclusion. *Popa v. Harriet Carter Gifts, Inc.*, 426 F. Supp. 3d 108, 123 (W.D. Pa. 2019).

but ultimately did not purchase anything. (ECF No. 93, ¶¶ 124–25); (ECF No. 105, ¶¶ 124–25). Although this interaction seems simple enough, it was simultaneously accompanied by various underlying communications between Popa's Safari web browser, Harriet Carter's website server, and a marketing technology company's—Navistone's—servers. It is from the interplay between these underlying communications that Popa brings this action alleging that "Harriet Carter procured Navistone to automatically and secretly spy on, and intercept, Harriet Carter's website visitors['] electronic communications with Harriet Carter in real-time." (ECF No. 38, ¶ 57). Popa alleges that both Harriet Carter and Navistone violated § 5703 of WESCA because Navistone unlawfully intercepted her communications with Harriet Carter. (ECF No. 38, ¶¶ 53–66).

Navistone is a marketing and technology company with offices located in Cincinnati, Ohio, servicing clients throughout the United States that collectively operate websites in the national marketplace. Navistone provides its clients—primarily e-commerce retailers—with services that allow them to send direct mail promotions to people visiting their websites. One of those clients is Harriet Carter.[2] Navistone provided Harriet Carter with customized JavaScript code that allowed various pages of Harriet Carter's website to gather and send information regarding website visitors directly to Navistone's servers located in Virginia. (ECF No. 93, ¶¶ 1–3, 6–7, 35); (ECF No. 105, ¶¶ 1–3, 6–7, 35).

The decision in this case requires a basic, layman's understanding of what happens when someone visits and peruses Harriet Carter's website (like Popa did) while Navistone's JavaScript code is operating. The interaction begins with a visitor navigating to Harriet Carter's website in one way or another (usually by clicking a link or searching the address). Once this occurs, the

[2] Harriet Carter's servers are located in Allentown, Pennsylvania. (ECF No. 105, ¶ 185); (ECF No. 108, ¶ 185).

visitor's web browser sends an HTTP GET request to Harriet Carter's web server. Harriet Carter's web server then responds by sending HTML to render on the visitor's web browser. After receiving the HTML, the visitor's web browser interprets various files required to view the website, including HTML, JavaScript, and CSS. (ECF No. 105, ¶ 198); (ECF No. 108, ¶ 198).

For purposes of this case, HTML controls the content of the website, CSS controls the appearance of the website, and GET requests are the primary mechanisms used for data retrieval on the internet. (ECF No. 105, ¶¶ 199–201); (ECF No. 108, ¶¶ 199–201). GET requests are physical, electrical signals on a wire, and sending and receiving data occurs nearly instantaneously. (ECF No. 105, ¶¶ 202–203); (ECF No. 108, ¶¶ 202–203).

When the visitor's web browser receives the HTML from Harriet Carter's web server, it is also instructed to send a GET request to Navistone to ask for the JavaScript code. Navistone's servers then respond by sending the JavaScript to the visitor's web browser, which then interprets the code on the visitor's device. (ECF No. 105, ¶ 198); (ECF No. 108, ¶ 198). At this point, the visitor's device will have successfully loaded Harriet Carter's web page.

After Harriet Carter's webpage has been received and fully rendered by the visitor's web browser, Navistone's JavaScript code begins collecting categories of information from the loaded webpage. The JavaScript code transmits a "payload" of information by sending GET requests to Navistone's servers each time the visitor loads a webpage, clicks on an "add to shopping cart" button, or if a "change event" relating to certain form fields occurs—for example, when a visitor tabs out of a form field or types what appears to be an email address in the form field. (ECF No. 93, ¶¶ 45–47, 55–57); (ECF No. 105, ¶¶ 45–47, 55–57). All information collected and sent by the JavaScript code is sent to Navistone's servers in Virginia in the form of raw data. (ECF No. 93, ¶ 66); (ECF No. 105, ¶ 66). To associate this raw information with website visitors, Navistone

places two cookies on the visitor's web browser after it has successfully rendered Harriet Carter's website. These cookies are anonymous/pseudonymous identifiers. The first-party cookie is an identification specific to Harriet Carter and is set under the domain of Harriet Carter's website, and the third-party cookie is one that remains the same for the visitor's browser across all Navistone's clients' websites. (ECF No. 105, ¶¶, 211–15); (ECF No. 108, ¶¶ 211–15). The exact information collected or Navistone's activities after receiving that information are immaterial to the resolution of the motion for summary judgment.

II. STANDARD OF REVIEW

Summary judgment is proper if "the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." FED. R. CIV. P. 56(a). *See also Celotex Corp. v. Cattrett*, 477 U.S. 317, 322 (1986). A fact is material if it must be decided in order to resolve the substantive claim or defense to which the motion is directed. In other words, there is a genuine dispute of material fact "if the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). The Court must view the evidence presented in the light most favorable to the nonmoving party. *Id.* at 255. It refrains from making credibility determinations or weighing evidence. *Id.* "Real questions about credibility, gaps in the evidence, and doubts as to the sufficiency of the movant's proof," will defeat a motion for summary judgment. *El v. Se. Pa. Transp. Auth.*, 479 F.3d 232, 238 (3d Cir. 2007). However, a mere "scintilla of evidence," without more, will not give rise to a genuine dispute for trial. *Saldana v. Kmart Corp.*, 260 F.3d 228, 232 (3d Cir. 2001).

III. ANALYSIS

Defendants ask the Court to enter summary judgment in their favor on Popa's remaining cause of action under WESCA. The questions presented in this case undoubtedly have the potential to broadly impact the manners and methods by which individuals and entities collect and transmit information across web platforms in Pennsylvania. Resolving whether an interception occurred within the meaning of WESCA, and whether any interception of communications occurred in Pennsylvania rests within the intricate communicative interplay between Popa's Safari web browser, Harriet Carter's web server, and Navistone's servers. After carefully considering the arguments and submissions of the parties, the Court holds that summary judgment is warranted. As a matter of law, there was no interception within the meaning of 18 Pa. C.S. § 5703, and even if there was, the communications at issue fall outside the scope of WESCA because they were received outside of Pennsylvania.

A. There Was Not an Interception of Information Under § 5703 Because Navistone Was a Direct Party to the Communications at Issue.

The threshold consideration in any claim arising under WESCA is whether there was an interception of communications. Defendants argue that there was not an interception of communications because any communications between the parties occurred separately and directly (i.e., between Popa and Harriet Carter, and between Popa and Navistone). (ECF No. 88, pp. 12–16). Popa contends that Defendants' position is without consequence because neither the statutory framework nor case law allows for an exclusion where an individual is a party to the communications at issue. (ECF No. 104, pp. 12–13).

The circumstances of this case are unique, and neither the parties' nor the Court's own research revealed Pennsylvania appellate authority applying § 5702's definition of intercept to communications sent and received between a user's web browser, a website's server, and third-

party servers. The Court's threshold inquiry of whether an interception occurs under these circumstances is a matter of first impression in Pennsylvania.

"When ascertaining Pennsylvania law, the decisions of the Pennsylvania Supreme Court are the authoritative source." *Spence v. ESAB Group, Inc.*, 623 F.3d 212, 216 (3d Cir. 2010) (citation omitted). "In the absence of a controlling decision by the Pennsylvania Supreme Court, [a district court] must predict how it would rule if faced with the issue." *Id.* (citation omitted).

> In making such a prediction, "[a district court] must look to decisions of state intermediate appellate courts, of federal courts interpreting that state's law, and of other state supreme courts that have addressed the issue," as well as to "analogous decisions, considered dicta, scholarly works, and any other reliable data tending to convincingly show how the highest court in the state would decide the issue at hand."

Id. at 216–17 (quoting *Norfolk S. Ry. Co. v. Basell USA Inc.*, 512 F.3d 86, 92 (3d Cir. 2008)). A district court must apply the state laws regardless of its views of its merits, and it should neither impose its own view of what the law should be, nor expand the law in ways outside of established state precedent. *Id.* at 217 (citations omitted).

Pennsylvania's General Assembly has provided a civil cause of action under WESCA, by which an aggrieved individual may institute an action to impose liability upon an offending party if the offending party:

> (1) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic or oral communication;
>
> (2) intentionally discloses or endeavors to disclose to any other person the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication; or
>
> (3) intentionally uses or endeavors to use the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know, that the information was obtained through the interception of a wire, electronic or oral communication.

18 Pa. C.S. §§ 5703 (1)–(3), 5725(a)(1)–(3). Pennsylvania's General Assembly defined an interception as follows:

> **"Intercept."** Aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device. The term shall include the point at which the contents of the communication are monitored by investigative or law enforcement officers . . . .

18 Pa. C.S. § 5702 (2020). While the statutory definition of "intercept" is silent on the specific type of communications at issue here, a series of Pennsylvania cases offer interpretations of that term which guide the Court's judgment here.

In *Commonwealth v. DiSilvio*, 335 A.2d 785 (Pa. Super. 1975), the appellant challenged the admissibility of evidence obtained by police during a raid of his operations under WESCA. *Id.* at 786. After detectives forced entry into the area, three telephones continued to ring, and upon the officers answering of some of those calls, the callers proceeded to place bets. *Id.* The appellant was later indicted and found guilty of pool selling and bookmaking. *Id.* The Superior Court of Pennsylvania held that there was no interception within the meaning of WESCA:

> Since the conduct of the officers in the instant case did not involve recording the conversation or the use of any electronic device for overhearing, we need only consider whether their activity constituted such an interception under the act as would require the consent of the parties to the communication. The officers here simply answered the telephones and spoke directly with the callers. In our view, this is not what was intended by the legislature to constitute an interception. *The callers freely elected to talk to the officers, whether or not they were informed of the identity and occupation of the recipients of the calls. By receiving the communication directly over the means of transmission employed, the officers were in fact themselves parties to the call.* Thus, no interception occurred, and the testimony of the officers as to their conversations is admissible.

Id. at 390–91 (citations omitted) (emphasis added).

In *Commonwealth v. Proetto*, 771 A.2d 823 (Pa. Super. 2001), a detective was alerted by a minor that an online predator was present in a chat room. *Id.* at 827. The detective entered the chat room under the name "Kelly15F" and began conversing with the predator. *Id.* After the

online predator made several unlawful suggestions, the detective made a log of the chat and had the predator arrested. *Id.* The defendant sought to suppress the evidence against him, claiming that it was garnered in violation of WESCA. The Superior Court again held that neither eavesdropping nor wiretapping occurred because there was not an "interception" of any information:

> First, we find that the Pennsylvania Wiretapping and Electronic Surveillance Act is not applicable to these communications. There was no "interception" in this case. Detective Morris, as "Kelly15F" was the intended recipient of these communications. This Court has held that *where a party receives information from a communication as a result of being a direct party to the communication, there is no interception.*
> . . . .
>
> In this case, Detective Morris was *a direct party to the communications from Appellant. There was no eavesdropping or wiretapping. Detective Morris obtained the information because he was a party to the communication.* The fact that Detective Morris did not identify himself as a police officer is of no effect . . . . Appellant freely elected to talk to Detective Morris, regardless of whether he was informed of "Kelly15F"'s true identity. Therefore the communications received by Detective Morris should not be suppressed on the grounds that the means of obtaining this information was in violation of the Act.

Id. at 831–32 (citations omitted) (emphasis added). *See also Vaughn v. Unemployment Compensation Bd. of Review*, No. 2471 C.D. 2011, 2012 WL 8704753, at *4 (Pa. Common. Sep. 10, 2012) (applying *Proetto* in a civil unemployment case and holding that there was no interception where an unemployment benefits claimant left an inappropriate voicemail with a customer because the customer was "the intended and actual recipient of the message, [and] simply forwarded [the] [c]laimant's message to third parties.").

Shortly after, the Supreme Court of Pennsylvania adopted and affirmed this rationale in *Commonwealth v. Cruttenden*, 619 A.3d 95 (Pa. 2012). The appeal in *Cruttenden* concerned "whether a police officer violate[d] . . . [WESCA] when he communicate[d] directly with a suspect via cell phone text messages while pretending to be the suspect's accomplice." *Id.* at 95–96. The

Pennsylvania Supreme Court held that the rule enunciated by *Proetto* was correct, and that an interception does not take place where an individual is a direct party to the communication:

> the underlying basis of the holding in *Proetto* was that no interception occurred and no eavesdropping or listening in on a conversation took place because the detective was a direct party to the communication. That a police officer *does not identify him- or herself, or misrepresents his or her identity, does not change the fact that he or she is a direct party to the conversation, and by virtue of being a direct party to the conversation, is deemed the intended recipient of the conversation* under whatever identity the officer has set forth.
>
> An officer is deemed the "intended recipient" of a phone communication in which the officer is directly involved, even under circumstances in which the officer shields or misrepresents his or her identity, because the caller elects to talk to the officer who answered the phone. The applicability of the Act does not rest on whether the caller's presumption of the identity of the person answering the call is accurate. It makes no difference instantly that Trooper Houk posed as Amodeo; the fact which takes the case out of the purview of the Act is that Appellee Lanier elected to communicate with the person answering the call and that the communication was direct. Therefore, there was no eavesdropping or listening in, and no interception took place.

Id. at 100 (citations omitted) (emphasis added).[3]

---

[3] *Cruttenden* and *Proetto* interpreted and applied the definition of intercept as stated by the Court *supra* at page 7. *Proetto*, 771 A.2d at 828–29; *Cruttenden*, 619 A.3d at 98 n.4. Pennsylvania's General Assembly seems to have agreed with *Proetto's* rationale, both factually and substantively, because, on October 25, 2012, it amended the definition by adding a third sentence, which excluded from the term

> the acquisition of the contents of a communication made through any electronic, mechanical or other device or telephone instrument to an investigative or law enforcement officer, or between a person and an investigative or law enforcement officer, where the investigative or law enforcement officer poses as an actual person who is the intended recipient of the communication . . . .

18 Pa. C.S. § 5702 (2012) (*as amended by* Act No. 2012-202, H.B. 2400, Regular Session 2011-2012 § 5702 (2012)) (current version at 18 Pa. C.S. § 5702 (2020)). Both parties have presented the definition of intercept by omitting the third sentence above (ECF No. 92, p. 12); (ECF No. 104, p. 10), and the Court agrees that the only relevant portion of the statute for purposes of resolving whether an interception occurred lies within the first two sentences because this case does not include communications made to law enforcement or investigative officers. And regardless of the General Assembly's amended addition, *Cruttenden*, *Proetto*, and *DiSilvio* remain authoritative and instructive because they interpreted and applied the definition of intercept (i.e., the first two

The cases above definitively provide that an interception does not occur where a party elects to speak with or send messages to a recipient because the recipient acquires the information contained in the communications by virtue of being a direct party to the communication. While this may be true, because this is a civil case that does not concern the more ordinary forms of communication dealt with by *Cruttenden*, *Proetto*, and *DiSilvio*—phone calls and typed-out electronic messages—their principles are not neatly applied to the unique technical circumstances here, and doing so requires a thorough understanding of the communicative interplay between the parties' respective technologies. Because WESCA's definition of an "interception," in pertinent part, is synonymous with the Federal Wiretap Act's definition of an "interception," *Proetto*, 771 A.2d at 829 (citations omitted), and the parties likewise agree that the Court "may look to decisions applying the ECPA for those provisions that mirror the ECPA, such as the definitions of intercept, contents, and electronic communications[,]" (ECF No. 104, p. 10 n.13); (ECF No. 115, p. 2), the United States Court of Appeals for the Third Circuit's reasoned analysis in *In re Google Inc.*

---

sentences) as it stood prior to the additional amendment, of which the Court is only dealing with here. *See Pa. State Police, Bureau of Liquor Control Enforcement v. Jet-Set Restaurant, LLC*, 191 A.3d 817, 823 (Pa. 2018) (citing 1 Pa. C.S. § 1922(4)) ("[W]here this Court has previously interpreted certain statutory language, and that language is retained in subsequent amendments to the same statute, the legislature approved of and intended to uphold that interpretation."); *Verizon Pa., Inc. v. Commonwealth*, 127 A.3d 745, 757 (Pa. 2015) ("One of the most venerable and fundamental tenets of statutory interpretation is that, whenever our Court has interpreted the language of a statute, and the General Assembly subsequently amends or reenacts that statute without changing that language, it must be presumed that the General Assembly intends that our Court's interpretation become part of the subsequent legislative enactment."); *Parisi v. Philadelphia Zoning Bd. of Adjustment*, 143 A.2d 360, 363 (Pa. 1958) (same); *In re Buhl's Estate*, 150 A. 86, 87 (1930) (same). *See* also *Commonwealth v. Shaffer*, 734 A.2d 840, 844 (Pa. 1999) ("once this Court interpreted the legislative language contained in the applicable act, our interpretation became part of the legislation from the date of its enactment."); *In re Lock's Estate*, 244 A.2d 677, 683 (Pa. 1968) (citation omitted) ("It has been held, and rightly so, that where a decision of the Superior Court construing a statute was never modified by the Supreme Court, the presumption was that when the legislature subsequently enacted a similar statute dealing with same subject matter, the legislature intended the same construction to be placed on the language of the subsequent statute.").

Cookie Placement Consumer Privacy Litigation, 806 F.3d 125 (3d Cir. 2015), is instructive of the communicative relationship between a visitor's web browser, the server of the visited website, and the third-party servers of advertising companies.[4]

In *In re Google*, the technologies corresponded and communicated with each other by sending and receiving GET requests containing certain information. *Id.* at 130. The Third Circuit detailed the process as follows:

> The host website leaves part of its webpage blank where the third-party advertisements will appear. Upon receiving a "GET" request from a user seeking to display a particular webpage, the server for that webpage will subsequently respond to the browser, instructing the browser to send a "GET" request to the third-party company charged with serving the advertisements for that particular webpage . . . . The third-party server responds to the GET request by sending the advertisement to the user's browser, which then displays it on the user's device. The entire process occurs within milliseconds and the third-party content appears to arrive simultaneously with the first-party content so that the user does not discern any separate GET requests from the third-parties.

Id. (footnote omitted). At the same time, in order for the internet advertising companies to successfully associate the users with their respective informational GET requests, the advertising companies would place third-party cookies on users' devices, which would allow the companies to associate users with their activities:

> To inject the most targeted ads possible, and therefore charge higher rates to buyers of the ad space, these third-party companies . . . compile the [i]nternet histories of users. The third-party advertising companies use "third-party cookies" to accomplish this goal. In the process of injecting the advertisements into the first-party websites, the third-party advertising companies also place third-party cookies on user's computing devices. Since the advertising companies place advertisements on multiple sites, these cookies allow these companies to keep track of and monitor

---

[4] Popa attempts to distinguish *In re Google* from the instant matter largely because she claims that, unlike § 2511(2)(d) of the ECPA, Pennsylvania has not expressly included a party exception under WESCA. (ECF No. 104, pp. 12 – 15). That distinction is without consequence because, as *Cruttenden*, *Proetto*, and *DiSilvio* explicitly recognized, a threshold interception under WESCA does not occur where a party receives information from a communication as a result of being a direct party to the communication.

> an individual user's web activity over every website on which these companies inject ads.
>
> These third-party cookies are used by advertising companies to help create detailed profiles on individuals . . . by recording every communication request by that browser to sites that are participating in the ad network, including all search terms the user has entered. The information is sent to the companies and associated with unique cookies—that is how the tracking takes place. The cookie lets the tracker associate the web activity with a unique person using a unique browser on a device. Once the third-party cookie is placed in the browser, the next time the user goes to a website with the same [d]efendant's advertisements, a copy of that request can be associated with the unique third-party cookie previously placed. Thus the tracker can track the behavior of the user . . . .

Id. at 131 (footnotes omitted).

Under the circumstances described in the complaint, the Third Circuit concluded that the users' web browsers and the servers of the internet advertising companies were communicating directly by sending and receiving information regarding the visited webpages. *Id.* at 140–41. To that extent, "there [was] no need for the defendants to acquire . . . information from transmissions to which they are not a party[] [because] [they] would have the information at issue anyway." *Id.* This conclusion was further supported by the defendants' direct placement of third-party cookies from their servers to visitors' web browsers because cookies only allowed the companies to associate information with particular users:

> Just as the operative allegations in the complaint tend to support the inference that the cookies enabled the defendants to identify, and thus associate, information that the plaintiffs sent directly to them in the ordinary course, the operative allegations tend to negate any inference to the contrary. This is because, if the information at issue was not sent to the defendants in the ordinary course, mere identification cookies would not be sufficient for the defendants' scheme. To accomplish their tracking in that instance, the defendants would have needed not an associative device, but one capable of capturing communications sent by the plaintiffs and intended for first-party websites, and then transmitting them to the defendants.

Id. at 141 (footnote omitted). Accordingly, because the users' web browsers directly communicated with the servers of the internet advertising companies, the Third Circuit held there

could be no violations of the ECPA because § 2511(2)(d)'s party exception precluded any interception where the individual is a party to the communication:

> Because the defendants were the intended recipients of the transmissions at issue—i.e. GET requests that the plaintiffs' browsers sent directly to the defendants' servers—we agree that § 2511(2)(d) means the defendants have done nothing unlawful under the Wiretap Act. Tautologically, a communication will always consist of at least two parties: the speaker and/or sender, and at least one intended recipient. As the intended recipient of a communication is necessarily one of its parties, and the defendants were the intended recipients of the GET requests they acquired here, the defendants were parties to the transmissions at issue in this case. And under § 2511(2)(d), it is not unlawful for a private person "to intercept a wire, oral, or electronic communication where such person is a party to the communication."

Id. at 142–43 (quoting 18 U.S.C. § 2511(2)(d)) (footnote omitted).

The processes and operations underlying the communications between a user's web browser, Harriet Carter's website server, and Navistone's servers are materially similar to those discussed in *In re Google*. The visitor's browser first sends a GET request to Harriet Carter's web server, and that server responds by sending HTML to the user's device. The user's device then interprets the requested HTML and sends a GET request to Navistone's server, and Navistone's server provides the requested JavaScript code together with cookies. After this point, the user's web browser transmits "payloads" of information regarding the user's activities on Harriet Carter's website by sending GET requests to Navistone's servers. (ECF No. 105, ¶ 198); (ECF No. 108, ¶ 198).

The information regarding certain activities of Popa on Harriet Carter's website was sent directly to Navistone via a GET request, and as a result, Navistone was a direct party to that information. In other words, the communications at issue in this case were directly between two parties to the conversation. As such, there was no interception.

Popa nevertheless argues that the principles enunciated in *Proetto* are distinguishable from the circumstances of this case because there was not a "secret-third party" in *Proetto*—there was only the police officer and defendants communicating directly in a chat room. (ECF No. 104, p. 13). She argues that *Proetto* is materially different because the sender in that case was at least aware that he was communicating with the recipient and intended to communicate with the recipient. (ECF No. 104, p. 13). In other words, Popa appears to argue that because she was unaware that she was communicating directly with Navistone, she did not freely elect to engage in the communications.

The Supreme Court and Superior Courts of Pennsylvania's holdings in *DiSilvio*, *Proetto*, and *Cruttenden* held that the appellants in each of those cases elected to engage in the communications with the recipient, regardless of who that recipient was. Those cases, however, were dealing with markedly different communicative media, which involved the sending and receiving of communications in their traditional sense—dialing a phone number and speaking with someone and typing out a message and sending it to someone. This case concerns the autonomous, and nearly instantaneous, sending and receiving of communications between a visitor's web browser and other web servers.

Although it was, of course, easier for the parties in *Cruttenden*, *Proetto*, and *DiSilvio* to understand that they were electing to begin or participate in a conversation because they were sending the messages or speaking into phones, there is one critical point of similarity: much like how the individuals in those cases chose to begin or participate in communications, Popa freely chose to visit Harriet Carter's website. By choosing to visit the website, she initiated the underlying communications between her web browser, Harriet Carter's web server, and Navistone's servers. In that sense, although she may have been unaware of the nuanced intricacies

required to build the webpage she requested, she nevertheless commanded her web browser to load the webpage, and her web browser carried out her command by sending and receiving information to and from various servers. From this perspective, understanding that our technical circumstances are not entirely comparable with *Cruttenden's*, *Proetto's*, or *DiSilvio's*, Popa's position is, in essence, the same. She communicated information to recipients without understanding their identities, which under *Cruttenden*, is inconsequential. That her web browser is requesting and receiving from various servers (Harriet Carter's and Navistone's) communications containing different bits of information, does not change the fact that she freely initiated the entire process, and upon doing so, her web browser carried out her request by directly beginning and participating in the ensuing "conversations."

Drawing all reasonable inferences in favor of Popa, judgment is warranted as a matter of law under § 5703 because Popa directly communicated with Navistone by visiting Harriet Carter's website—thereby commanding her web browser to communicate with various servers to build the requested website—and Navistone was privy to those communications by virtue of being a direct party. There was, therefore, no interception. The Court will grant summary judgment in favor of Defendants.

B. Even If an Interception Did Occur, Navistone Is Not Liable Under WESCA Because It Acquired the Information Outside of Pennsylvania.

Defendants argue in the alternative that, even if an interception did occur, they would not be liable for that interception under WESCA because it occurred outside of Pennsylvania—the information was received in Virginia and interpreted in Ohio. (ECF No. 88, pp. 16–18). Popa argues, however, that the information was intercepted in Pennsylvania where it originated. (ECF No. 104, pp. 18–19). As the Court previously set forth in its December 6, 2019, Memorandum Opinion (ECF No. 59), Pennsylvania's appellate courts have "refused to extend WESCA to out-

of-state conduct." *Popa v. Harriet Carter Gifts, Inc.*, 426 F. Supp. 3d 108, 115 (W.D. Pa. 2019) (citing *Larrison v. Larrison*, 750 A.2d 895, 898 (Pa. Super. 2000)). The Court, however, declined to resolve issues surrounding the location and timing of the interception on a motion to dismiss because the record at that time was insufficiently developed. *Id.* at 116.

The appropriate starting point is rooted in the General Assembly's definition of the term "intercept," which is defined as "[a]ural or *other acquisition of the contents* of any wire, electronic or oral communication . . . ." 18 Pa. C.S. § 5702 (2020) (emphasis added). Because this case does not concern aural acquisition, the Court's inquiry is primarily focused on what it means to otherwise acquire the contents of a communication. Framed in this manner, resolution of the issue rests on the point at which Navistone acquired the contents of any communications. To that extent, the point of acquisition must have occurred within Pennsylvania for WESCA to impose liability upon Navistone.

The General Assembly did not define the term "acquisition" in 18 Pa. C.S. § 5702, and the Court will therefore apply the canons of the Statutory Construction Act, 1 Pa. C.S. §§ 1501–1991. *Commonwealth v. Wise*, 171 A.3d 784, 788 (Pa. Super. 2017). In Pennsylvania, "[t]he plain language of the statute is generally the best indicator of legislative intent, and the words of a statute 'shall be construed according to the rules of grammar and according to their common and approved usage . . . .'" *Commonwealth v. Hall*, 80 A.3d 1204, 1211 (Pa. 2013) (quoting 1 Pa. C.S. § 1903(a)). Because of the former, only when words are unclear or ambiguous, or the plain meaning would lead to a result that is absurd, impossible of execution, or unreasonable, should courts look beyond the plain language. *Id.* (citing 1 Pa. C.S. § 1922(1)). The term "acquisition," in the ordinary sense, is generally defined as "the act of acquiring something[,]" and "acquire" is defined as "to get as one's own[.]" *Acquisition*, MERRIAM WEBSTER'S DICTIONARY, https://www.merriam-

webster.com/dictionary/acquisition (last visited May 17, 2021); *Acquire*, MERRIAM WEBSTER'S DICTIONARY, https://www.merriam-webster.com/dictionary/acquire (last visited May 17, 2021).

The Court agrees with Defendants that if an interception did occur, no factfinder could reasonably conclude that the interception occurred in Pennsylvania because the communications were only obtained by Navistone after the visitor's web browser sent that information via GET request to Navistone's servers in Virginia. This is because information is being generated in a pre-recorded format, and then being sent and received by the parties. If the code were to malfunction by failing to send the GET request, Navistone would not receive any information surrounding the visitor's activities. With this in mind, Navistone does not "acquire" any communications according to that term's common and approved usage because Navistone cannot make something its own (i.e., acquire something) that it does not receive. As a result, because Navistone does not acquire any communications pertaining to a website visitor's interactions with Harriet Carter's website until it receives the contents of those communications via GET request, Navistone did not acquire the communications at issue until they reached its servers in Virginia. Thus, the only "acquisitions" present in this case occurred outside the Commonwealth and, consequently, the scope of WESCA.

As a matter of law, Navistone is not subject to liability under WESCA because it acquired the communications at issue in Virginia. The Court will grant summary judgment in favor of Defendants.

IV. CONCLUSION

For the reasons set forth above, the Court will grant summary judgment in favor of Defendants on Count I of the Amended Complaint. Orders of Court will follow.

BY THE COURT:

WILLIAM S. STICKMAN IV
UNITED STATES DISTRICT JUDGE

6.17.2021
Dated