2026 PA Super 236

RAELEEN THOMPSON, INDIVIDUALLY AND BEHALF OF ALL THOSE SIMILARLY SITUATED Appellant v. C. & J. CLARK AMERICA, INC.	:	IN THE SUPERIOR COURT OF PENNSYLVANIA No. 74 WDA 2026

Appeal from the Order Entered December 5, 2025
In the Court of Common Pleas of Washington County Civil Division at No(s): 2023-1326

BEFORE: BOWES, J., OLSON, J., and MURRAY, J.

OPINION BY MURRAY, J.: **FILED: OCTOBER 23, 2026**

Raeleen Thompson (Appellant) appeals from the order entering summary judgment against her and in favor of C. & J. Clark America, Inc. (Clarks or Clarks America). After careful review, we vacate and remand for further proceedings.

On February 14, 2023, Appellant filed a putative class action complaint against Clarks, a footwear retailer, asserting claims for violations of Pennsylvania's Wiretapping and Electronic Surveillance Control Act (WESCA), 18 Pa.C.S.A. §§ 5701-5782, and common law invasion of privacy. Appellant alleged that Clarks, via third-party vendors, "wiretapp[ed] the electronic communications of visitors to its website, www.clarksusa.com [(hereinafter "the website," "Clarks website," or "Clarks America website")]," including

"their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications…." Complaint, 2/14/23, ¶ 1. After Clarks filed preliminary objections, the trial court dismissed Appellant's common law invasion of privacy claim, and Appellant proceeded solely on her WESCA claim.

Relevantly, section 5703 of WESCA provides as follows:

> Except as otherwise provided in this chapter, a person is guilty of a felony of the third degree if he:
>
> (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.A. § 5703. Section 5702 defines "Intercept" as follows:

> 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. The term shall not include 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, provided that the Attorney General, a deputy attorney general

> designated in writing by the Attorney General, a district attorney or an assistant district attorney designated in writing by a district attorney of the county wherein the investigative or law enforcement officer is to receive or make the communication has reviewed the facts and is satisfied that the communication involves suspected criminal activities and has given prior approval for the communication.

Id. § 5702; ***see also id.*** (defining "Electronic communication" as "Any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system…."; and defining "Contents" as follows: "As used with respect to any wire, electronic or oral communication, is any information concerning the substance, purport, or meaning of that communication.").

Section 5704 ("Exceptions to prohibition of interception and disclosure of communications") provides, in pertinent part, that "[i]t shall not be unlawful and no prior court approval shall be required under this chapter for … [a] person, to intercept a wire, electronic or oral communication, **where all parties to the communication have given <u>prior consent</u> to such interception**." ***Id.*** § 5704(4) (emphasis added).

Section 5725 establishes a civil cause of action for WESCA violations, providing as follows:

> **(a) Cause of action.**--Any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication; and shall be entitled to recover from any such person:

> (1) Actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of violation, or $1,000, whichever is higher.
>
> (2) Punitive damages.
>
> (3) A reasonable attorney's fee and other litigation costs reasonably incurred.

Id. § 5725(a).

Instantly, on June 13, 2024, Clarks filed an answer and new matter to Appellant's complaint. The parties thereafter engaged in and completed discovery. On July 15, 2025, Clarks filed a motion for summary judgment. Appellant subsequently filed a response in opposition to the motion, and the trial court heard oral argument. On December 5, 2025, the trial court filed a memorandum opinion and order, granting the motion and entering summary judgment in Clarks' favor.

In its opinion, the trial court set forth the underlying facts, indicating that it viewed the record in the light most favorable to Appellant. ***See*** Trial Court Opinion, 12/5/25, at 3. The trial court summarized Appellant's experience with the Clarks website as follows:

> Sometime "probably" in 2022, [Appellant] first visited the Clarks America website. Clarks' Motion for Summary Judgment (MSJ), 7/15/25, Exhibit A (Appellant's Deposition Transcript) at 19. She did so by using her S23 Galaxy phone. When she accessed the Clarks America website, she was in her home and estimates that the time of year was "probably spring going into summer." ***Id.*** at 20. [Appellant's] purpose was to "see what sandals were coming out." ***Id.*** at 21. [Appellant] recalls using a Google search to navigate to the Clarks America website. ***Id.*** at 22.
>
> While on the Clarks America website, [Appellant] did not share any of her personally identifiable information. She did not

enter her name, her email or any credit card information. She did not create an account with Clarks America. Other than searching for sandals, [Appellant] did not share any information regarding her browsing history, previous queries, personal interests or habits. She does not remember clicking on a particular pair of sandals. She did not use the "chat function" on the site. ***Id.*** at 23-26.

[Appellant] returned to the Clarks America website a second time "probably" in either 2023 or in July of 2024. ***Id.*** at 8. She once again employed a Google search on her phone to browse the Clarks America website. She typed the word "sandals" into the search bar, used a filter function for sizes, and looked at the inventory in her size. ***Id.*** at 29-32.

Similar to her first visit, [Appellant] provided no other information. She did not use the "chat function." She did not share any of her personal information to include her name, email address, credit card information or home address. She did not create an account. ***Id.*** at 33-34.

After these visits, [Appellant] received "pop-up" ads "targeting" her to look at other "Clark[s] items." She described receiving Clarks pop-up ads on Facebook. When using Google and typing in "something similar" she would be directed to the Clarks America website.[1] In other words, she observed previous searches being auto-populated. ***Id.*** at 36-39. Other than her interest in sandals, she does not believe that any other "sensitive" information was captured. ***Id.*** at 40.

[Appellant] did not see or search for the Clarks America terms of use. ***Id.*** at 70-71. She did not review the "cookie" policy on the Clarks America website. She confirmed that prior to 2024[,] she did not disallow "cookie[s]" that tracked her browsing activity on the Clarks website. ***Id.*** at 75-76.

Nevertheless, [Appellant] asserts she was harmed when Clarks America tracked what she looked at on the Clarks website and then later sent her ads about sandals that she was not

---

[1] Ironically, Appellant testified that she became a class representative in the instant lawsuit only after she saw a "pop-up [ad] on Facebook" from the law firm that now represents her, which stated "[t]here was a possible class action lawsuit against Clarks…." Appellant's Deposition Transcript at 17-18.

> interested in buying. ***Id.*** at 76. She maintains that her time was wasted because "Clarks" was always showing up as the first website in her search for sandals. ***Id.*** at 77-80.

Trial Court Opinion, 12/5/25, at 3-5 (original footnote citations moved to body and modified; footnote added).

The trial court next summarized the record evidence regarding data tracking on the Clarks website:

> During the time periods when [Appellant] browsed the Clarks America website, Content Square, a Paris[-]based company, provided optimization services to Clarks America. Appellant's Response to MSJ, 8/22/25, Exhibit A (January 26, 2021, Agreement between Clarks and Content Square). Through [its] agreement [with Clarks], Content Square guaranteed a "tracking service level" of 99.9% for each month. ***Id.*** at Appendix 5. Content Square also agreed to process personal data from website and mobile app visitors for Clarks America's website. The personal data included: IP addresses, cookie ID's, "other similar unique identifiers;" the pages of the website the visitor visited; the visitor's type of computer operating system; the type of web browser used by a visitor; and behavioral information concerning the visitor. Such behavioral information concerned "how a visitor interacted with the website[,]" … includ[ing "]mouse or touch movements, scrolls, mouse clicks, screen taps, zoom information, and the time of engagement." ***Id.*** at Annex 1.
>
> [Appellant] retained an expert in network technology, Matthew Strebe [(Mr. Strebe), who submitted an expert report dated August 22, 2025]. Utilizing the "Wayback Machine,"[2] [Mr. Strebe] examined how tracking technology functioned on the Clarks America website. Appellant's Response to MSJ, 8/22/25, Exhibit C (Strebe Report) ¶ 4. …
>
> … Mr. Strebe states that Content Square's tracking code deploys immediately when a user loads the first webpage.

---

[2] "The Wayback Machine is an online digital archive of web pages. It is run by the Internet Archive, a nonprofit library in San Francisco, California." ***Valve Corp. v. Ironburg Inventions Ltd.***, 8 F.4th 1364, 1374 (Fed. Cir. 2021) (citation omitted).

> According to Mr. Strebe, even if a user were to go directly from Clarks America's homepage to its privacy policy page, Content Square would have already captured the user's request to go to the privacy page. Mr. Strebe added that Content Square's tracker ships information directly out of a user's browser and not from the web address for Clarks America. Mr. Strebe explained that Clarks America's website does not collect the information Content Square tracks. ***Id.*** ¶¶ 70, 82.
>
> Mr. Strebe opines that Content Square "unquestionably" captured the contents of [Appellant's] communications while she used the search query looking for sandals on the Clarks America website. ***Id.*** ¶ 67. He explained that Content Square also intercepted any clicks by [Appellant] on any particular type of sandals. According to Mr. Strebe, the capture of "hovers, clicks, specific page URLs" show the "intent and purport" of [Appellant's] communications with the Clarks website. ***Id.*** ¶ 68.
>
> As for [Appellant's] consent, Mr. Strebe offers that Clarks America's "Privacy Policy" does not apply to Content Square's activity. Mr. Strebe, a non-lawyer, points out that the "Privacy Policy" states that it applies only to information collected by www.clarksusa.com. Mr. Strebe reiterates that the data that Content Square intercepts is not collected by www.clarksusa.com. Mr. Strebe opines that Content Square intercepts 100% of a user's communications with the Clarks America website. ***Id.*** ¶¶ 69-71, 81.

Trial Court Opinion, 12/5/25, at 5-7 (original footnote citations moved to body and modified; one footnote added).

The trial court set forth the following legal analysis:

> [WESCA] emphasizes the protection of privacy and provides statutory remedies that extend to non-constitutional violations. ***Commonwealth v. Spangler***, 809 A.2d 234, 237 (Pa. 2002) (citing ***Commonwealth v. DeMarco***, 578 A.2d 942, 949 (Pa. Super. 1990)). "In general, [WESCA] prohibits the interception, disclosure or use of any wire, electronic or oral communication." ***Commonwealth v. Byrd***, 235 A.3d 311, 319 (Pa. 2020).
>
> However, [WESCA's] prohibitions give way to a mutual consent exception "where all parties to the communication have given prior consent to such interception." 18 Pa.C.S.A. § 5704(4);

see also Popa v. Harriet Carter Gifts, Inc., 52 F.4th 121, 132 (3d Cir. 2022) [(***Popa II***)[3]]; ***Byrd***, 235 A.3d 311. The mutual consent exception does not require express consent of a party to an interception. The Pennsylvania Supreme Court has made clear that "prior consent under the mutual consent exception is based on whether an individual knew or should have known they were being recorded." ***Byrd***, 235 A.3d at 313.

In circumstances where an interception of an electronic communication sent over the Internet occurs, the mutual consent exception applies. Writing for a unanimous Court [in ***Byrd***], Justice Mundy explained:

> ["B]y the very act of sending a communication over the Internet, the party expressly consents to the recording of the message." [***Commonwealth v. Cruttenden***, 58 A.3d 95, 98 (Pa. 2012)] (citing [***Commonwealth v.***] ***Proetto***, [771 A.2d 823,] 829 [(Pa. Super. 2001)]). Again, the objective reasonable person consents by proceeding with the communication knowing it will be recorded.

Byrd, 235 A.3d at 320. This approach to electronic communications is not new. ***Byrd*** is a capstone to a similar line of precedent coming from Pennsylvania's appellate courts.

---

[3] In ***Popa v. Harriet Carter Gifts, Inc.***, 544 F. Supp. 3d 535 (W.D. Pa. 2021) (***Popa I***), which involved a putative class action WESCA claim similar to Appellant's instant claim, the United States District Court for the Western District of Pennsylvania granted summary judgment in the defendants' favor. In ***Popa II***, the Third Circuit vacated the order granting summary judgment and remanded for further consideration. ***Popa II***, 52 F.4th 121. On remand, the district court followed the Third Circuit's guidance and again granted summary judgment. ***Popa v. Harriet Carter Gifts, Inc.***, 772 F. Supp. 3d 592 (W.D. Pa. 2025) (***Popa III***). Thereafter, on unrelated grounds involving lack of Article III jurisdiction, the Third Circuit vacated the summary judgment grant and remanded to the district court with instructions to remand the action to Pennsylvania state court. ***Popa v. Harriet Carter Gifts, Inc.***, No. 25-1760, 2026 WL 837280 (3d Cir. Mar. 26, 2026) (non-precedential opinion) (***Popa IV***). We discuss the ***Popa*** decisions at length below.

Trial Court Opinion, 12/5/25, at 7-8 (citations, capitalization, and paragraph breaks modified; original footnote omitted; footnote added).

The trial court discussed relevant caselaw as follows:

> [In ***Proetto***,] a police officer did not violate [WESCA] where he entered an Internet chat room under a fictitious name and struck up a conversation with a target chat room user. The target had been soliciting underage girls to engage in sexual conduct with him. ***Proetto***, 771 A.2d at 827. The Superior Court commented[,]
>
> > This situation is unlike one in which a party is engaging in a conversation over the telephone. While engaging in a conversation over the telephone, a party would have no reason to believe that the other party was taping the conversation. **Any reasonably intelligent person, savvy enough to be using the Internet, however, would be aware of the fact that messages are received in a recorded format, by their very nature, and can be downloaded or printed by the party receiving the message. By the very act of sending a communication over the Internet, the party expressly consents to the recording of the message.**
>
> ***Id.*** at 829 [(trial court's emphasis)].
>
> Eleven years later[, in ***Cruttenden***,] the Pennsylvania Supreme Court explained that ***Proetto*** maintained a long-held distinction in [WESCA] precedent. Namely, "the Superior Court held [in ***Proetto***] that [WESCA] was not violated because the officers were deemed to be direct parties to the [communication]." ***Cruttenden***, 58 A.3d at 100. The [***Cruttenden***] Court declared "it is irrelevant that an officer intentionally misrepresents his identity to the person with whom he communicates…." ***Id.*** at 96. ***Cruttenden*** involved a defendant who unwittingly sent text messages to a state trooper who was posing as his accomplice in an interstate drug transaction. The Court explained:
>
> > It makes no difference instantly that [the trooper] posed as [the accomplice]; the fact which takes the case out of the purview of [WESCA] is that [the

> defendant] 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.

Three years later, the Superior Court reiterated that "the applicability of [WESCA] does not rest on whether the … presumption of the identity … is accurate." ***Commonwealth v. Diego***, 119 A.3d 370, 380 (Pa. Super. 2015). In ***Diego***, an accomplice (Still) who had been arrested agreed to send text messages to his source of heroin (Diego). In the presence of a police officer, Still arranged for the purchase of heroin from Diego[,] with the transaction to be consummated at a [hotel]. The Superior Court ruled [that] "Still was a party to the conversation, and therefore[,] he could not be said to have intercepted it simply because he received it." ***Id.*** at 380-81. The Superior Court added[,] "[t]hat [Still] subsequently relayed the contents of that conversation to the police does not render either his or the police's conduct an 'interception' under the plain meaning of [WESCA]." ***Id.*** at 381.

Five years later[,] in ***Byrd***, the Supreme Court addressed an inmate's claim that he had to possess *actual knowledge* that his phone calls were being recorded in order for the mutual consent exception to apply. The Supreme Court rejected that argument. Justice Mundy stated

> the phrase "actual knowledge" does not appear in the statutory language of the mutual consent exception[,] and [the a]ppellant fails to argue any basis for its application as the standard. Rather, our case law illustrates that "prior consent" can be demonstrated when the person being recorded "knew[,] or should have known, that the conversation was being recorded." ***Diego***, 119 A.3d at 377.

Byrd, 235 A.3d at 319.

To summarize, certain basic principles apply to the mutual consent exception set forth in [WESCA]. First, a person need not have actual knowledge that his or her electronic communications are being recorded. ***Byrd***, ***supra***. Second, a person need not know the true identity of the recipient of the electronic

> communication. Indeed, a person may be deceived as to the identity of the person with whom he or she is communicating. ***Proetto***, ***Cruttenden***, and ***Diego***, ***supra***. Third, the "very act of sending a communication over the Internet" amounts to express consent to recording. ***Byrd***, 235 A.3d at 320; ***Proetto***, 771 A.2d at 829.

Trial Court Opinion, 12/5/25, at 8-10 (some citations modified).

Applying these principles to the instant case, the trial court concluded Appellant "may not proceed to trial," reasoning as follows:

> First, [Appellant] need not have actual knowledge nor have fully appreciated that her mouse or touch movements, scrolls, mouse clicks, screen taps, zoom information, and her time of engagement were being recorded. ***Byrd***, ***supra***. … Second, [Appellant] need not have known that Content Square, on behalf of Clarks America, was tracking her mouse or touch movements, scrolls, mouse clicks, screen taps, zoom information, and her time of engagement. ***Proetto***, ***Cruttenden***, and ***Diego***, ***supra***. Third, [Appellant's] "very act" of sending an electronic communication over the Internet amounted to her express consent to recording. ***Proetto***, 771 A.2d at 829.
>
> In other words, when [Appellant] surfed the Internet for summer sandals and clicked on the Clarks America website, she should have known that Clarks America or another acting on its behalf was tracking her activity on the Clarks America website. Under the Fourth Amendment, a person has no legitimate expectation of privacy in information that "he voluntarily turns over to third parties." ***Smith v. Maryland***, 442 U.S. 735, 743-44 (1979). Under the "third-party doctrine," a person who reveals his affairs to another has taken the risk that the information would be conveyed by that person to the government. ***See United States v. Miller***, 425 U.S. 435, 443 (1976).
>
> As discussed above, this trial court recognizes [WESCA] provides statutory relief that extends to non-constitutional violations. ***See Spangler***, 809 A.2d at 237. Nevertheless, the provisions of [WESCA] are strictly construed. ***See Boettger v. Miklich***, 633 A.2d 1146, 1148 (Pa. 1993). For that reason, Pennsylvania courts have been reluctant to []read in ["]specific

> requirements" that the legislature did not include in the language of [WESCA]. ***Spangler***, 809 A.2d at 241.
>
> Here, [Appellant] points to no specific provision of [WESCA] that requires her consent to tracking when she voluntarily chooses to click on an Internet website and browse. This court may not[,] by an act of judicial fiat[,] read in such a requirement. Further, this trial court may not depart from a strict construction of [WESCA's] mutual consent exception as informed by precedent from the Supreme and Superior Courts.

Trial Court Opinion, 12/5/25, at 10-11 (some citations and capitalization modified). The trial court therefore entered summary judgment against Appellant and in favor of Clarks.

Appellant timely appealed and filed a court-ordered Pa.R.A.P. 1925(b) concise statement of matters complained of on appeal. The trial court filed a statement in lieu of opinion under Rule 1925(a), indicating its reliance on its December 5, 2025, memorandum opinion.

Appellant presents the following questions for our review:

> 1. Did the trial court err in holding that [Appellant] gave express prior consent to being wiretapped by Content Square through her "very act" of sending an electronic communication to Clarks over the Internet?
>
> 2. Did the trial court improperly construe Content Square as an agent of Clarks and incorrectly believe that such status allowed Clarks to circumvent the all-party consent requirement in WESCA?
>
> 3. Did the trial court err in holding that [Appellant] failed to make a *prima facie* showing sufficient to allow a trier of fact to find that her communications with Clarks' website were unlawfully intercepted by Content Square?

Appellant's Brief at 5-6 (issues reordered).

When reviewing an order granting summary judgment, this Court's

> scope of review is plenary, and our standard of review is the same as that applied by the trial court. An appellate court may reverse the entry of a summary judgment only where it finds that the lower court erred in concluding that the matter presented no genuine issue as to any material fact[,] and that it is clear that the moving party was entitled to a judgment as a matter of law. In making this assessment, we view the record in the light most favorable to the nonmoving party, and all doubts as to the existence of a genuine issue of material fact must be resolved against the moving party. As our inquiry involves solely questions of law, our review is *de novo*.
>
> Thus, our responsibility as an appellate court is to determine whether the record either establishes that the material facts are undisputed or contains insufficient evidence of facts to make out a *prima facie* cause of action, such that there is no issue to be decided by the fact-finder. If there is evidence that would allow a fact-finder to render a verdict in favor of the non-moving party, then summary judgment should be denied.

Huggins v. Progressive Advanced Ins. Co., 359 A.3d 465, 467-68 (Pa. Super. 2026) (citation omitted).

We address Appellant's first two issues together, as they are related. In her first issue, Appellant argues the trial court erred in concluding she gave prior consent to Content Square's interception of her electronic communications with the Clarks website. Appellant's Brief at 19-26, 31-38. Appellant contends the trial court's reliance on ***Cruttenden*** and ***Proetto*** was misplaced, as "[t]hose cases did not involve real-time interceptions of website browsing; they only involved communications that were received by direct recipients in a recorded format." ***Id.*** at 20; ***see also id.*** at 34-38 (distinguishing ***Cruttenden*** and ***Proetto***). Appellant argues she did

> not complain[] of any recordings made by Clarks *itself*, nor did she allege that Content Square was able to record her

> communications by deceiving her and *posing* as Clarks. Instead, [Appellant] alleged—and her record evidence proves—that Clarks violated WESCA by procuring Content Square to *intercept* her communications with Clarks in real time, without her knowledge or prior consent, and by using those intercepted communications with reason to know they were obtained through a wiretap.

Id. at 20-21 (emphasis in original) (citing 18 Pa.C.S.A. § 5703(1), (3)).

Appellant asserts that

> [i]n interpreting and applying WESCA, it is crucial for courts to maintain a distinction between: 1) *a party* merely *receiving* a communication and sharing it after-the-fact; and 2) the *contemporaneous interception* of a communication *by a third party*. WESCA was specifically designed to prohibit the latter.
>
> Similarly, a recording made by a known participant to an Internet communication is distinguishable from the interception of an Internet communication by a third party whose eavesdropping is not known to all participants. WESCA defines the term "intercept" as the "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa.C.S.A. § 5702.
>
> This case is about a third-party interception—not after-the-fact disclosure by Clarks or a first-party recording by Clarks—but the trial court's opinion did not respect those distinctions in the statute or caselaw, leading it to apply inappropriate precedents.

Id. at 24-25 (footnote omitted; emphasis in original).

Appellant also argues that ***Byrd*** is distinguishable, as it "involved a recording of an oral conversation, and that recording was preceded by a conspicuous oral warning that the conversation could be recorded or monitored." ***Id.*** at 31; ***see also id.*** at 31-34 (distinguishing ***Byrd***). Appellant maintains that "[u]nlike the closed-circuit telephone system in ***Byrd***, no warning was issued when [Appellant] arrived on the [Clarks w]ebsite that the entirety of her visit might be 'monitored and recorded.'" ***Id.*** at 34.

Appellant acknowledges that ***Byrd*** recognized an objective standard, whereby "prior consent" under WESCA "can be demonstrated when the person being recorded 'knew, or should have known, that the conversation was being recorded.' This standard is one of a reasonable person, and not proof of the subjective knowledge of the person being recorded." ***Id.*** at 22 (quoting ***Byrd***, 235 A.3d at 319 (quoting ***Diego***, 11 A.3d at 377)). Appellant maintains it is undisputed that she "lacked *actual* knowledge that her communications to Clarks would be intercepted by Content Square." ***Id.*** at 23 (emphasis in original). She therefore asserts that "the remaining question before the trial court was whether Clarks' evidence showed … that a reasonable person in [Appellant's] position 'should have known,' before beginning her communications with Clarks, that the communications would be intercepted by a third-party eavesdropper—Content Square—as she made them." ***Id.*** (punctuation modified).

Appellant argues that Content Square's data tracking "was undisclosed by Clarks and imperceptible by ordinary Internet users," ***id.*** (citing Appellant's Deposition Transcript at 69-76); and "the only way for a … user to know that Content Square is receiving any transmissions during the browser session is with the use of advanced developer tools…." ***Id.*** at 34 (citing Mr. Strebe's Report ¶¶ 25, 45-46). Appellant maintains that "[a]t the very least, the question of what a reasonably intelligent person would understand about the

existence, functionality, and purposes of Content Square's Tracking Code upon arriving on the [Clarks w]ebsite is a question for the finder of fact, not for the trial court on a motion for summary judgment." ***Id.***

> Appellant asserts that the trial court's ruling,
>
> if upheld, means WESCA provides no privacy protections *whatsoever* on the Internet. The trial court's misuse of language from ***Proetto*** and ***Cruttenden*** resulted in the trial court's creation of a dramatic carveout of *all* Internet communications from WESCA's protection….

Id. at 41 (emphasis in original). Appellant maintains that, "[u]nder WESCA's text, it does not matter whether the contents of an electronic communication meet some subjective definition of 'sensitive' or 'private.'" ***Id.*** (citing ***Bartnicki v. Vopper***, 532 U.S. 514, 526 (2001) (recognizing that Pennsylvania's WESCA, like the federal Wiretap Act, "is in fact a content-neutral law of general applicability," and stating the federal Wiretap Act "does not distinguish based on the content of the intercepted conversations, nor is it justified by reference to the content of those conversations. Rather, the communications at issue are singled out by virtue of the fact that they were illegally intercepted—by virtue of the source, rather than the subject matter")).

In her second issue, Appellant argues the trial court erred in determining that she should have known that "Clarks America *or another acting on its behalf* was tracking her activity on the Clarks America website." ***Id.*** at 43 (quoting Trial Court Opinion, 12/5/25, at 11 (Appellant's emphasis)).

According to Appellant, the trial court "ruled that [Appellant's] knowledge that the recipient of her communications was recording her (Clarks) is the same as having knowledge that an unknown third party (Content Square) is intercepting her communications 'on [Clarks'] behalf.'" ***Id.*** at 43-44.

Appellant contends that the trial court treated Content Square as Clarks' agent, though "Clarks never alleged or argued that Content Square was its agent." ***Id.*** at 44. More importantly, Appellant argues, "the trial court's reference to an agency relationship between Clarks and Content Square was misguided because … WESCA does not allow third parties to intercept communications on a party to the communication's behalf." ***Id.*** at 45 (citing 18 Pa.C.S.A. § 5703(1) (prohibiting a person from "procur[ing] any other person to intercept or endeavor to intercept any wire, electronic or oral communication")). Appellant maintains the trial court's ruling "nullif[ies] either the 'procurement' prohibition or the all-party consent requirement, or both." ***Id.*** at 46 (citing ***Popa II***, 52 F.4th at 128). Appellant asserts, "[t]he trial court's treatment of Clarks and Content Square as if they were the same party … was directly at odds with the plain language of WESCA's protections." ***Id.*** at 47.

Clarks counters that the trial court properly determined that Appellant consented to the use of data tracking on the Clarks website. Clarks' Brief at 19-31. Clarks maintains that its website's

> Privacy Policy and Terms of Use clearly explained to website visitors the nature, type, and manner of information that the

> Clarks America Website collected and used in 2022. ***See*** MSJ, 7/15/25, Exhibit F (Privacy Policy). Indeed, they specifically informed visitors they should not visit the website if they do not want that information collected or used. ***See id.*** If visitors continued on the website, like [Appellant], they consented to that collection and use. ***See id.***

Clarks' Brief at 24 (record citations modified).

Clarks relies on ***Popa III***, in which the district court determined that the plaintiff gave constructive consent under WESCA to third-party data collection on a retail website, where the website's privacy policy adequately described the data collection and was reasonably conspicuous on the website. ***See id.*** at 23-27 (discussing ***Popa III***). Clarks maintains that its own Privacy Policy adequately described the alleged "interception" of users' communications with the website. ***Id.*** at 27 n.9. Clarks further maintains that the Privacy Policy's hyperlink was "conspicuous[ly]" located at the center and bottom of the webpage, such that Appellant, "or any other user, could have easily seen it and understood its contents." ***Id.*** (quoting ***Popa III***, 772 F. Supp. 3d at 606-07).

Clarks also argues that Appellant's claim fails because she

> did not provide any protected content. [Appellant] did not input any personally identifiable information in the Clarks America website during her 2022 visit. She did not input her name, address, date of birth, or phone number. She did not input any financial information, such as a credit card number or bank account information. She did not input any private health information. She did not use any sort of chat function on the website.
>
> Instead, [Appellant] typed the word "sandals" into the search bar on the Clarks America website. She then scrolled

> through the pictures of sandals. She did not remember whether she clicked on any of those pictures, but she did not select any for purchase. This is no different than browsing in a brick-and-mortar store. It is not actionable under [WESCA]. ***See*** [] ***Goldstein v. Costco Wholesale Corp.***, 559 F. Supp. 3d 1318, 1320-1321 (S.D. Fla. 2021) ("th[e] mere tracking of plaintiff's movements on defendant's website is the cyber analog to record information defendant could have obtained through a security camera at a brick-and-mortar store") (dismissing complaint alleging violation of the Florida Wiretap Act …).

Clarks' Brief at 27-28 (record citations omitted; some capitalization modified).

With respect to Appellant's second issue, Clarks argues that the trial court "did not … treat Clarks America and Content Square as if they were the same party or make the legal conclusion that Content Square was Clarks America's agent." ***Id.*** at 44. Rather, Clarks maintains, the trial court's determination that Appellant "should have known that Clarks America or another acting on its behalf was tracking her activity on the Clarks America website," ***id.*** (quoting Trial Court Opinion, 12/5/25, at 11), was consistent with undisputed record evidence that (1) Content Square provided "certain data-analytic tools for the … Clarks America website" pursuant to a contractual relationship; and (2) the website's Privacy Policy "explained that Clarks worked with third parties that track consumer behavior for the very purpose of sending targeted advertising." ***Id.*** at 44-45.

Initially, we observe that both the trial court and Appellant have cited the Third Circuit's decision in ***Popa II***, while Clarks relies on the district court's decision in ***Popa III***. ***See*** Trial Court Opinion, 12/5/25, at 7; Appellant's Brief at 30, 46-47; Clarks' Brief at 23-27. As the ***Popa*** decisions involve

substantially identical issues as the instant case, we find them highly instructive,[4] particularly given the lack of Pennsylvania caselaw applying WESCA to the precise circumstances at issue here. We therefore discuss the ***Popa*** decisions in some detail.

In ***Popa***, the plaintiff (Popa) filed a putative class action claim against a retailer (Harriet Carter) and a marketing technology company (Navistone), alleging they violated WESCA "by unlawfully intercepting her data while she shopped online." ***Popa I***, 544 F. Supp. 3d at 537. In ***Popa I***, the district court summarized the relevant factual 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 but ultimately did not purchase anything. 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." Popa alleges that both Harriet Carter and Navistone violated § 5703 of WESCA because Navistone unlawfully intercepted her communications with Harriet Carter.

---

[4] "We recognize that decisions of the … federal circuit courts are not binding upon this Court, but may serve as persuasive authority." ***Dobransky v. EQT Prod. Co.***, 273 A.3d 1133, 1146 n.10 (Pa. Super. 2022) (*en banc*) (citation omitted). Similarly, while "federal district court cases are not binding on this Court," we "may utilize the analysis in those cases to the extent we find them persuasive." ***Umbelina v. Adams***, 34 A.3d 151, 159 n.2 (Pa. Super. 2011) (citation omitted).

Id. (record citations omitted).

In ***Popa I***, the district court granted summary judgment in the defendants' favor, concluding that no "interception" occurred under WESCA. ***See id.*** at 539-46. After discussing ***Cruttenden***, ***Proetto***, and ***Commonwealth v. DiSilvio***, 335 A.2d 785 (Pa. Super. 1975), the district court determined these decisions "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." ***Popa I***, 544 F. Supp. 3d at 543. The district court then reviewed "the communicative interplay between the parties' respective technologies," and determined that Navistone was a direct party to the communications at issue. ***Id.*** at 543. The district court reasoned as follows:

> 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*** [***Inc. Cookie Placement Consumer Privacy Litigation***, 806 F.3d 125 (3d Cir. 2015)]. The visitor's browser first sends a[n HTTP] 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.
>
> 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 I, 544 F. Supp. 3d at 545 (record citations omitted).

Popa appealed to the Third Circuit, which vacated the district court's summary judgment grant. ***Popa II***, 52 F.4th at 133. After reviewing WESCA's text and relevant Pennsylvania caselaw, the ***Popa II*** Court determined "there is no sweeping direct-party exception to civil liability under WESCA." ***Id.*** at 129. The Third Circuit observed that ***Proetto*** and ***Cruttenden*** held that no "interception" occurred where a police officer was the direct recipient of a communication, even where the officer misrepresented his identity. ***Id.*** at 126-27. However, the Third Circuit noted that, in 2012, the General Assembly amended WESCA and "explicitly included as a carve-out in the definition of 'intercept'" situations wherein a "law enforcement officer … acquir[es] communications when he is an 'intended recipient' or … pos[es] as one[.]" ***Id.*** at 128 (quoting 18 Pa.C.S.A. § 5702 ("The term [(intercept)] shall not include the acquisition of the contents of a communication made … 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….")). The Third Circuit reasoned that the General Assembly's "deci[sion] to codify a specific, narrow intended-recipient exemption for" police—matching "the specific facts and holdings of ***Proetto*** and ***Cruttenden***"—implied the General Assembly's "reject[ion]" of

the "broader," potentially "expansive reach of those cases," and therefore, the amendment "limit[ed] ***Proetto*** and ***Cruttenden*** to their facts." ***Id.***

Interpreting section 5704(4)'s all-party consent exception, the Third Circuit reasoned that if "a party to a communication may lawfully intercept it without the other person's consent just because it is a 'direct party' to that communication, the all-party consent requirement would disappear." ***Id.*** at 128. The Third Circuit determined that direct-party liability must be considered through the lens of consent, with section 5704(4) permitting interception of communications in instances where the sender "knew, or should have known, that the conversation was recorded." ***Id.*** at 129 (quoting ***Diego***, 119 A.3d at 377). Thus, the Third Circuit concluded the defendants "cannot avoid liability merely by showing that Popa unknowingly communicated directly with Navistone's servers." ***Id.*** It additionally concluded that "an interception occurred" when Popa's communications were routed to Navistone's servers. ***Id.*** at 131.

The ***Popa II*** Court then addressed the issue of Popa's consent, noting the defendants

> argue Popa impliedly consented to the interception because Harriet Carter included a privacy policy on the website when she visited. Though Popa claims she never saw the policy, the Pennsylvania Supreme Court has said that "prior consent" in § 5704(4) does not require "actual knowledge." … ***Byrd***, … 235 A.3d [at] 319…. Prior consent, including implied consent, "can be demonstrated when the person being recorded knew or should have known[] that the conversation was being recorded." ***Id.*** (internal quotation marks omitted).

> Because the district court granted summary judgment on other grounds, it never addressed whether Harriet Carter posted a privacy policy and, if so, whether that policy sufficiently alerted Popa that her communications were being sent to a third-party company. The defendants assert the privacy policy adequately alerted a reasonable person to the interception; hence Popa's conduct using the Harriet Carter website demonstrated she consented. Popa disagrees that the policy went far enough and, alternatively, contends there is a genuine issue of material fact about whether this policy even existed at the time she visited the Harriet Carter website.

Popa II, 52 F.4th at 132 (some capitalization modified). Noting "there are unresolved disputes about the evidence supporting the [d]efendants' privacy policy arguments," the Third Circuit remanded to the district court for a determination as to "whether the [d]efendants are entitled to summary judgment on the basis of Harriet Carter's privacy policy." ***Id.*** at 132-33.

On remand, the parties engaged in additional discovery, and the defendants again moved for summary judgment. ***Popa III***, 772 F. Supp. 3d at 596. In ***Popa III***, the district court summarized the record with respect to Harriet Carter's privacy policy:

> 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. It is not disputed that at all times relevant to this case, Harriet Carter had a privacy policy posted in the footer of its website. The privacy policy was presented as a link, labeled "Privacy Statement." The link was in white, against a blue background. The parties, including their experts, agree that presenting a link to a privacy policy in the footer of a website was the common practice for commercial websites in 2018. The parties further agree that in 2018, it would have been a "reasonable conclusion" for a company to believe that "it ought to put the privacy policy link in the footer of its website."

The Harriet Carter privacy policy ("Privacy Statement") broadly address its practices with respect to collection and use of customer information collected from its website. Under the heading "When I visit HarrietCarter.com, what information is gathered about me and why?" the Privacy Statement states, *inter alia*, "Harriet Carter does collect certain customer information. We use this information to process orders, enhance your shopping experience and communicate with our customers." The Privacy Statement has a section entitled "What are Cookies and Should I Worry About Them?" that explains what cookies are and how they are used in connection with the Harriet Carter website. It explains, for example, that "[o]ur site does use cookies to keep track of your shopping cart. We also use cookies to help make your shopping experience more enjoyable[,] and if you choose to register with us or request to receive email, we will use cookies to deliver content specific to your interests." The Privacy Statement has a section that addresses the access of third parties to customer information. The heading states, in bold type: "Who Else Has Access to the Information I provide to Harriet Carter.com?" It states, in relevant part:

> We may from time to time contract with third party vendors to serve ads to our customers on our behalf across the Internet or to send our catalogs to customers whom we think may be interested in our products or services. To do this, the vendors will collect anonymous information about your visits to our Web site and your interaction with our products and services. This anonymous information is collected through the use of a cookie or pixel tag—industry standard technology used by most major Web sites. No personally identifiable information is collected in this process. They may also pool the anonymous information that they collect with other sources of information not collected during your visit to our website, which may include your name and mailing address.

In Popa's deposition, she testified that she has never reviewed the Privacy Statement … [and] that, as a matter of practice, she does not review [websites'] privacy policies….

Id. at 597-98 (record citations omitted).

Relying on ***Byrd***, ***Proetto***, and ***Diego***, the district court recognized that "Pennsylvania courts have repeatedly interpreted the consent provisions of WESCA as establishing an objective standard—looking to whether a reasonably prudent person can be deemed to have consented under the circumstances." ***Popa III***, 772 F. Supp. 3d at 601. Regarding the reasonable person standard, the district court further stated as follows:

> While not expressly addressing WESCA, but relevant to the reasonable person standard, the Third Circuit has made observations about the expectation of privacy in internet activity that [are] consistent with ***Proetto***. In ***In re Nickelodeon Consumer Priv. Litig.***, 827 F.3d 262, 266 (3d Cir. 2016), the Third Circuit observed:
>
> > Most of us understand that what we do on the Internet is not completely private. How could it be? We ask large companies to manage our email, we download directions from smartphones that can pinpoint our GPS coordinates, and we look for information online by typing our queries into search engines. We recognize, even if only intuitively, that our data has to be going somewhere. And indeed it does, feeding an entire system of trackers, cookies, and algorithms designed to capture and monetize the information we generate. Most of the time, we never think about this. We browse the Internet, and the data-collecting infrastructure of the digital world hums along quietly in the background.
>
> ***In re Nickelodeon***, 827 F.3d at 266. Contrary to [d]efendants' argument that the nature of the internet itself warrants a finding of implied consent to interception under WESCA, and respectful of the Third Circuit's observation [in ***Popa II***] that ***Nickelodeon*** is distinguishable because of WESCA's two-way consent requirement, the [district c]ourt finds the above-quoted language instructive on the reasonable person standard used to examine implied consent under WESCA. It recognizes that, while the nature of the internet does not confer blanket implied consent to interception under WESCA, a reasonably prudent person has a

> lower expectation of privacy on the internet than on, for example, a telephone, which lacks the "entire system of trackers, cookies, and algorithms" commonly, if not ubiquitously, implicated in the use of a website. Like the [Superior C]ourt in ***Proetto***, the [district c]ourt believes that when determining whether a reasonable person can be deemed to consent to an interception under WESCA, it must be mindful of the reality of internet communication and expectations of ordinary people in interacting with the internet.

Popa III, 772 F. Supp. 3d at 602-03.

Turning to Harriet Carter's Privacy Statement, the district court reasoned, "In order for a privacy statement to convey consent to an interception, it must disclose the nature of the interception to a reasonable reader. … Not unlike the disclosure of the recording in ***Byrd***, the question is whether a reasonable person *could* have been apprised of the complained-of activity." ***Id.*** at 603 (italics in original). The district court held that Harriet Carter's "Privacy Statement adequately discloses that third parties, like Navistone, may have access to information relating to consumers' activities on the website." ***Id.*** The district court determined that the Privacy Statement "makes clear that Harriet Carter uses cookies on its website and that those cookies may track users' activities"; "includes language that unequivocally reveals that Harriet Carter may share information about users' activities with third parties"; and "provides sufficient information to alert a reasonably prudent visitor to the Harriet Carter website of the critical issue for a WESCA claim—that third parties, like Navistone, may collect data relating to the visitor's conduct on the website." ***Id.*** at 603, 604.

Next, acknowledging the record did not show Popa had actual knowledge of the Privacy Statement's terms, the district court considered "whether a reasonable person in her circumstance could be charged with implicit knowledge of the disclosures in the Privacy Statement. This turns on the visibility and accessibility of the Privacy Statement to an ordinary user." ***Id.*** at 604. The district court outlined the relevant legal principles as follows:

> The question of whether a reasonable person would have had sufficient notice of Harriet Carter's Privacy Statement follows the type of analysis commonly employed by courts to determine whether a user assented to a website's contractual terms and conditions by continued use of the website. Courts have recognized that there are two general methods of posting terms and conditions on a website:
>
> > Contracts formed on the Internet come primarily in two flavors[:] "clickwrap" (or "click-through") agreements, in which website users are required to click on an "I agree" box after being presented with a list of terms and conditions of use; and "browsewrap" agreements, where a website's terms and conditions of use are generally posted on the website via a hyperlink at the bottom of the screen.
> >
> > "Unlike a clickwrap agreement, a browsewrap agreement does not require the user to manifest assent to the terms and conditions expressly … [a] party instead gives his assent simply by using the website."
>
> ***Nguyen v. Barnes & Noble Inc.***, 763 F.3d 1171, 1175-76 (9th Cir. 2014) (quoting ***Hines v. Overstock.com, Inc.***, 668 F. Supp. 2d 362, 366-67 (E.D.N.Y. 2009)). "A 'browsewrap agreement' allows the user 'to view the terms of the agreement but does not require the user to take any affirmative action before the Web site performs its end of the contract.'" ***Freeplay Music, LLC v. Dave Arbogast Buick-GMC, Inc.***, No. 3-17-CV-42, 2019 WL 4647305, at *10 (S.D. Ohio Sept. 24, 2019) (internal citations omitted). It is undisputed that Harriet Carter's Privacy Statement took the

> form of a browsewrap agreement and, while it was visible and accessible, visitors were not required to click or otherwise express affirmative consent to its terms.
>
> Courts consistently enforce browsewrap agreements when users have actual notice. ***Nguyen***, 763 F.3d at 1176; ***see also Register.com Inc. v. Verio, Inc.***, 356 F.3d 393, 401 (2d. Cir. 2004); ***Ticketmaster Corp. v. Tickets.com, Inc.***, 2003 WL 21406289, at *1 (C.D. Cal. Mar. 7, 2003). If there is no evidence of actual knowledge, the enforceability of a browsewrap agreement turns on whether the website placed a reasonably prudent user on inquiry notice of its terms. ***Nguyen***, 763 F.3d at 1177 (citing ***Specht v. Netscape Common's Corp.***, 306 F.3d 17, 30 (2d Cir. 2002)). The content of a webpage and privacy agreement page determine whether a defendant adequately provides inquiry notice. ***Id.*** (citing ***Be In, Inc. v. Google, Inc.***, 2013 WL 5568706, at *1 (N.D. Cal. Oct. 9, 2013)).
>
> Courts have generally held that "constructive knowledge alone is sufficient to establish consent to 'browsewrap' terms and conditions when the website host placed the notice of the terms and agreements 'prominently' and provided 'easy access' to the full terms." ***Freeplay Music***, 2019 WL 4647305, at *11 (quoting ***Snap-On Bus. Sols. Inc. v. O'Neil & Assocs., Inc.***, 708 F. Supp. 2d 669, 682 (N.D. Ohio 2010)). Citing to the Ninth Circuit's decision in ***Nguyen***, the Third Circuit has explained that "[t]here is an evolving body of caselaw regarding whether the terms and conditions in browsewrap agreements are enforceable, often turning on whether the terms or a hyperlink to the terms are reasonably conspicuous on the webpage." ***James v. Global Tellink Corp.***, 852 F.3d 262, 267 (3d Cir. 2017) (internal citations omitted). The Third Circuit observed that such terms will likely not be enforced "[w]hen terms are in obscure sections of a webpage that users are unlikely to see." ***Id.*** (citing ***Specht***, 306 F.3d at 30-32). The Second Circuit similarly observed that "clarity and conspicuousness" of terms are "important in securing informed consent." ***Nicosia v. Amazon.com, Inc.***, 834 F.3d 220, 233 (2d Cir. 2016); ***see also Meyer v. Uber Technologies, Inc.***, 868 F.3d 66, 75-76 (2d Cir. 2017) (same).

Popa III, 772 F. Supp. 3d at 604-05.

Applying these principles to the record before it, the district court held that

> the Privacy Statement on Harriet Carter's website was "reasonably conspicuous on the webpage" so as to charge Popa with "'constructive notice' that continued use [constituted] acceptance of the agreement." ***HealthplanCRM*** [***LLC. V. AvMed, Inc.***], 458 F. Supp. 3d [308,] 331 [(W.D. Pa. 2020)] (quoting ***James***, 852 F.3d at 267). It is undisputed that, at the time relevant to this case, Harriet Carter had a hyperlink labeled "Privacy Statement" in the footer of every page of its website. The hyperlink was in white font contrasting against a blue background. In addition to this location at the center and bottom of each page, a link to the privacy statement could be found in the drop-down menu on the left side of the website directly below "Email Us." The [district c]ourt holds that, based on the appearance and layout of Harriet Carter's website, the Privacy Statement was reasonably conspicuous. It was not, for example, linked in "obscure sections of a webpage that users are unlikely to see." ***HealthplanCRM***, 458 F. Supp. 3d at 332 (citing ***James***, 852 F.3d at 267). Nor were the relevant terms concerning the policy, as the arbitration clause in ***HealthplanCRM***, included in a hyperlink generically labeled "terms of use" or the like. Rather the link was specifically labeled "Privacy Statement." Popa, or any other user, could have easily seen the link and understood exactly what it contained.
>
> The record also establishes that the placement and appearance of the Privacy Statement on the Harriet Carter website was in line with common usage in 2018. Popa's own expert testified that it was common for privacy policies to be placed on the footer of the websites…. To be clear, whether Harriet Carter's manner of displaying its Privacy Statement was commonplace in 2018 is not independently dispositive. It is, however, instructive. Where the manner of posting a privacy policy was consistent with common industry practice, and the appearance of the language was visible and not hidden in an obscure place on the website, a court should [be] … hesitant to find that the posted terms were incapable of conveying constructive notice.
>
> When viewing the record as a whole, the [district c]ourt holds that the Privacy Statement is enforceable. Popa's decision not to review its terms does not permit her to avoid the implication of those terms. The hyperlink to the Privacy Statement was

> reasonably conspicuous. It was displayed in a white contrasting font against a blue background on the bottom of every page of the website[.[5]]
>
> Further, … the title of the Privacy Statement [hyperlink] gave an express indication of the contents of the hyperlink. The Privacy Statement adequately discloses that third parties, such as Navistone, may access information relating to user activities on Harriet Carter's website. The [district c]ourt holds that these factors compel a finding that a reasonable person in Popa's position had constructive notice of the terms of the Privacy Statement as a matter of law. As in ***Byrd***, the [district c]ourt holds that Popa constructively consented to any interception effectuated by Navistone.[6] There was, therefore, no violation of

---

[5] The ***Popa III*** opinion included a screenshot of Harriet Carter's website, ***Popa III***, 772 F. Supp. 3d at 607, which showed the hyperlink to the "Privacy Statement, in white font against the blue background, … circled in red at the footer of the website." ***Id.*** at 607 n.5.

[6] The ***Popa III*** court

> reject[ed] Popa's contention that the presence of Navistone's program means that merely visiting Harriet Carter's website would give rise to an actionable interception under WESCA before she, or any reasonable user, had a chance to view the terms of the Privacy Statement. This argument is incorrect. To the extent that Popa was concerned about privacy, she could have immediately reviewed the Privacy Statement and, if concerned, left the page. This is no different than if someone who received the warning in ***Byrd*** hung up the phone after hearing the recording. The mere fact that a user visits Harriet Carter's website is not protected by WESCA any more than that of a caller who uses a phone to reach a number, and then hangs up after being warned of an interception and/or recording. The caller's number may show up, and even be recorded, on a caller identification system, but an intercept has not occurred. WESCA only applies to "contents" of communications, which it defines as "information concerning the substance, purport, or meaning of that communication." 18 Pa.C.S.[A.] § 5702. Accessing the Harriet Carter webpage, visiting the Privacy Statement, and then leaving the site does not lead to the interception of "content" under WESCA.

Popa III, 772 F. Supp. 3d at 608 n.6.

> WESCA and summary judgment in [the d]efendants' favor is warranted.

Popa III, 772 F. Supp. 3d at 606-08 (record citations and footnotes omitted; footnotes added).

Popa again appealed to the Third Circuit, which again vacated the district court's summary judgment grant, albeit on jurisdictional grounds unrelated to ***Popa III***'s substantive analysis. ***Popa IV***, 2026 WL 837280 at *1-2 (non-precedential opinion). The Third Circuit explained that

> [w]hile this appeal was pending, we addressed our Article III jurisdiction in a similar case, ***Cook v. GameStop, Inc.***, 148 F.4th 153 (3d Cir. 2025) [(involving a putative class action claim for alleged WESCA violations relating to data tracking on a retail website)]. There, we held that a plaintiff who "moved her mouse, clicked links, typed in a search bar, and added a product to her 'cart,'" but "did not input any sensitive or personal information" did not suffer a sufficiently concrete injury-in-fact. ***Id.*** at 156, 162. Consistent with ***GameStop***, we conclude—as Popa concedes—that she did not suffer a "cognizable Article III harm[]" sufficient to avail herself of federal jurisdiction. So we will vacate and remand with instructions for the [d]istrict [c]ourt to remand the action to state court.

Popa IV, 2026 WL 837280, at *1 (non-precedential opinion) (record citation omitted). We observe that the jurisdictional defect which resulted in ***Popa III***'s vacatur, *i.e.*, the lack of an existing case or controversy, is not relevant to the questions before us, and the ***Popa IV*** decision does not signify any disapproval of ***Popa III***'s substantive analysis.[7]

---

[7] In her reply brief, Appellant faults Clarks for citing ***Popa III*** without mentioning that the decision had been subsequently vacated by ***Popa IV***. *(Footnote Continued Next Page)*

We agree with the analysis of both ***Popa II*** and ***Popa III***, and consider their reasoning persuasive with respect to the instant appeal.

Instantly, the trial court determined that when Appellant visited the Clarks website, "Content Square … was tracking her mouse or touch movements, scrolls, mouse clicks, screen taps, zoom information, and her time of engagement." Trial Court Opinion, 12/5/25, at 10. The trial court further determined that Appellant "need not have actual knowledge nor have fully appreciated" that her communications with the Clarks website "were being recorded," nor that Content Square was performing that recording on Clarks' behalf. ***Id.*** Rather, the trial court concluded that Appellant's "'very act' of sending an electronic communication over the Internet amounted to her express consent to recording." ***Id.*** (quoting ***Proetto***, 771 A.2d at 829). "In other words, when [Appellant] surfed the Internet for summer sandals and clicked on the Clarks America website, she should have known that Clarks

---

Appellant's Reply Brief at 23-24. Appellant argues that "when a reviewing court vacates an opinion of a lower court, it 'deprives that court's opinion of precedential effect.'" ***Id.*** at 24 (quoting ***O'Connor v. Donaldson***, 422 U.S. 563, 577 n.12 (1975)). Appellant maintains that, "[f]or this reason alone, this Court should disregard Clarks' arguments in reliance o[n] ***Popa*** [***III***]." ***Id.*** However, we reiterate that decisions of the federal circuit courts and district courts are not binding on this Court, and we consider them for their persuasiveness, not their precedential effect. ***See Dobransky***, 273 A.3d at 1146 n.10; ***Umbelina***, 34 A.3d at 159 n.2. ***Popa III***'s vacatur on jurisdictional grounds unrelated to the issues before us does not diminish its persuasive value for our present purposes.

America or another acting on its behalf was tracking her activity on the Clarks America website." ***Id.*** at 11.

We agree with the trial court that the record, viewed in the light most favorable to Appellant, establishes a genuine issue of material fact that Content Square tracked Appellant's communications with the Clarks website. Though the trial court did not explicitly characterize this tracking as an "interception" under WESCA, the court determined Appellant consented to the tracking, and Appellant's consent would not be necessary unless an interception occurred. Trial Court Opinion, 12/5/25, at 10; ***see also*** 18 Pa.C.S.A. § 5704(4) (all-party consent exception).[8] As the alleged tracking here appears to be materially indistinguishable from that involved in ***Popa***, we conclude said tracking would constitute an interception under WESCA for the same reasons set forth in ***Popa II***. ***See*** 18 Pa.C.S.A. § 5702 (defining "intercept"); ***Popa II***, 52 F.4th at 126-32; ***Popa I***, 544 F. Supp. 3d at 545 (discussing the "processes and operations underlying the communications" at issue in ***Popa***).

---

[8] Despite its determination that Appellant consented to the tracking, the trial court also stated that Appellant "points to no specific provision of [WESCA] that requires her consent to tracking when she voluntarily chooses to click on an Internet website and browse." Trial Court Opinion, 12/5/25, at 11. However, section 5704(4), which the trial court purported to apply, sets forth the all-party consent exception to the unlawfulness of an interception under WESCA. 18 Pa.C.S.A. § 5704(4).

We further agree with the trial court that, regarding consent, Appellant "need not have actual knowledge" of the tracking, and that the relevant question is whether Appellant "should have known" about the tracking. Trial Court Opinion, 12/5/25, at 10, 11. In determining prior consent under WESCA section 5704(4), we apply a reasonable person standard: whether a reasonable Internet user in Appellant's position knew or should have known that the contents of her communications with the Clarks website would be acquired by a third party. ***See Popa II***, 52 F.4th at 132 ("Prior consent, including implied consent, 'can be demonstrated when the person being recorded knew or should have known[] that the conversation was being recorded.'" (quoting ***Byrd***, 235 A.3d at 319)).

However, to the extent that the trial court applied this standard, it painted with too broad a brush. First, the trial court overextended the reach of ***Proetto*** and ***Cruttenden*** when it made the blanket statement that, with respect to WESCA's all-party consent exception, "a person need not know the true identity of the recipient of the electronic communication" and, "[i]ndeed, … may be deceived as to the identity of the person with whom he or she is communicating." Trial Court Opinion, 12/5/25, at 10 (citing ***Proetto*** and ***Cruttenden***). In our view, whether the identity of the recipient and/or the interceptor is relevant to the sender's consent must be determined by applying a reasonable person standard to the circumstances at issue.

In ***Proetto*** and ***Cruttenden***, defendants who were engaged in criminal activity communicated with police officers who had misrepresented their identities to the defendants. In ***Proetto***, this Court determined police did not obtain the defendant's chat messages in violation of WESCA because the defendant "freely elected to talk to [the officer], regardless of whether he was informed of [the recipient's] true identity." ***Proetto***, 771 A.2d at 832. In ***Cruttenden***, our Supreme Court held that, under WESCA, "it is irrelevant that an officer intentionally misrepresents his identity to the person with whom he communicates." ***Cruttenden***, 58 A.3d at 96. As the ***Popa II*** Court explained, subsequent amendments to WESCA excepted from the definition of "intercept" a situation wherein a police officer "poses as an actual person who is the intended recipient of the communication…." 18 Pa.C.S.A. § 5702 (effective Dec. 24, 2012); ***see also Popa II***, 52 F.4th at 127-28.

We do not interpret these authorities as establishing a principle that, for the purposes of consent under section 5704(4), it is *never* relevant that the sender does not know, or is deceived about, the identity of the recipient and/or the interceptor. We note that ***Proetto*** and ***Cruttenden*** involved police officers, and the amended definition of "intercept" specifically licensed only police officers to "pose[]" as another person. 18 Pa.C.S.A. § 5702. Thus, misrepresenting one's identity in order to receive communications appears to

be a prerogative belonging to police officers.[9] Further, we observe that even where police officers have been licensed to misrepresent their identities, this license applies only where the police officer "poses as … **the intended recipient** of the communication." 18 Pa.C.S.A. § 5702 (emphasis added). In both ***Proetto*** and ***Cruttenden***, the defendant and the officer were the only parties to the communication, and the officer posed as the intended recipient. Neither case involved interception or eavesdropping by a third party, and neither stands for the proposition that it is irrelevant that the sender of a communication is unaware of the involvement of a third-party interceptor.

Here, Appellant emphasizes that she did not "complain[] of any recordings made by" the intended recipient of her communications (Clarks), "nor did she allege that Content Square was able to record her communications by deceiving her and *posing* as Clarks." Appellant's Brief at 20 (emphasis in original). Appellant maintains "that Clarks violated WESCA by procuring Content Square," an unknown third party, "to intercept her communications with Clarks." We agree with Appellant that, contrary to the trial court's determination, the holdings of ***Proetto*** and ***Cruttenden***, regarding deception as to the recipient's identity, do not control in this

---

[9] We observe that even police officers do not have unfettered license under WESCA to pose as another person, but may do so only where "the Attorney General, … a district attorney," or their designee "has reviewed the facts and is satisfied that the communication involves suspected criminal activities and has given prior approval for the communication." 18 Pa.C.S.A. § 5702.

situation. Rather, we determine that a reasonable person standard must be applied to the circumstances at issue. ***See Byrd***, 235 A.3d at 319.

Next, the trial court again overextended ***Proetto*** in determining that Appellant's "'very act' of sending an electronic communication over the Internet amounted to her express consent to recording." Trial Court Opinion, 12/5/25, at 11 (quoting ***Proetto***, 771 A.2d at 829). We observe that ***Proetto*** involved a defendant who sent Internet chat room messages to a minor child (who subsequently turned the messages over to police) and, separately, to a police officer posing as a minor child. ***Proetto***, 771 A.2d at 826-27. In determining that no WESCA violation occurred when the minor child received the defendant's messages and later turned them over to police, the ***Proetto*** Court stated as follows:

> This situation is unlike one in which a party is engaging in a conversation over the telephone. While engaging in a conversation over the telephone, a party would have no reason to believe that the other party was taping the conversation. **Any reasonably intelligent** person, savvy enough to be using the Internet, however, would be aware of the fact that **messages are received in a recorded format, by their very nature**, and can be downloaded or printed **by the party receiving the message**. By the very act of sending a communication over the Internet, the party expressly consents to the recording of **the message**.

Id. at 829 (emphasis added).

First, we note this statement involves the ***Proetto*** Court's determination as to what a reasonable Internet user should know about the nature of chat room messages. Proper application of this principle to a different form of Internet communication, such as an Internet shopper's interaction with a retail

website, would require a determination as to what a reasonable person should know about that form of communication. Second, ***Proetto*** did not conclude that a reasonable person sending a message consents to the recording of the message by someone other than the intended recipient. We reiterate that neither ***Proetto*** nor ***Cruttenden*** (which relied on ***Proetto***'s above-quoted language) involved more than two parties to the communication, and the contents of the defendants' messages were acquired by either the intended recipient or a police officer posing as the intended recipient.

In short, ***Proetto*** and its progeny do not support the trial court's blanket ruling, which implies that any person sending any form of communication over the Internet inherently consents to the acquisition of that communication's contents by anyone who happens to be listening/recording. Such a determination divorces the ***Proetto*** Court's broad language regarding "the very act of sending a communication over the Internet" from its essential context, which involved determining what a reasonable person sending a chat room message should know about the nature of that particular form of communication. The trial court's conclusion that Appellant "should have known that Clarks America **or another acting on its behalf** was tracking her activity on the Clarks America website," Trial Court Opinion, 12/5/25, at 11 (emphasis added), was rendered without an apparent application of the reasonable person standard to the particular form of Internet communication at issue; nor did the trial court consider whether a reasonable person should

be aware that someone other than the intended recipient may be acquiring the contents of the communication.

Clarks does not explicitly defend the trial court's broad ruling, but rather urges us to rely on its website's privacy policy (the Privacy Policy) in affirming the trial court's conclusion that Appellant consented to the data tracking at issue. ***See*** Clarks' Brief at 19-31. Appellant counters that the trial court did not rely on the Privacy Policy, and contends that Clarks seeks affirmance on alternative grounds. Appellant's Reply Brief at 24-26. However, "[i]t is well settled that this Court may affirm the decision of the trial court if it is correct on any grounds." ***Liberty Mut. Ins. Co. v. Domtar Paper Co.***, 77 A.3d 1282, 1286 (Pa. Super. 2013) (citing ***Lilliquist v. Copes-Vulcan, Inc.***, 21 A.3d 1233, 1235 (Pa. Super. 2011), for the proposition "that an appellate court may affirm a trial court's decision on any grounds supported by the record on appeal"); ***see also Cassel-Hess v. Hoffer***, 44 A.3d 80, 85 (Pa. Super. 2012) (determining trial court erred in granting summary judgment on trespass claim based upon lack of standing, but affirming grant of summary judgment on other grounds (citing ***Lilliquist***, 21 A.3d at 1235)). Thus, the trial court's lack of reliance on Clarks' Privacy Policy does not bar us from considering Clarks' argument that the Privacy Policy supports affirmance.[10]

---

[10] We observe that while "we have the ability to affirm a decision on any grounds that are supported by the record,"

(Footnote Continued Next Page)

We agree with the ***Popa II*** Court's rationale that a website's privacy policy is relevant to the question of what a reasonable Internet user should know about third-party data acquisition on the website. ***Popa II***, 52 F.4th at 132-33. We further find persuasive the ***Popa III*** court's determination that, based on Harriet Carter's privacy policy, Popa implicitly consented under section 5704(4) to Navistone's acquisition of the contents of her communications with Harriet Carter's website. ***Popa III***, 772 F. Supp. 3d at 600-08. We will therefore consider whether the instant record supports a similar determination with respect to Clarks' Privacy Policy.

> since a trial court cannot "raise an argument in favor of summary judgment *sua sponte* and grant summary judgment thereon," it would appear as if this Court—also—cannot affirm a trial court's grant of summary judgment upon an argument that was never raised in support of the summary judgment motion. ***See Yount v. Pa. Dep't of Corr.***, 600 Pa. 418, 966 A.2d 1115, 1119 (2009) ("[f]or a trial court to raise an argument in favor of summary judgment *sua sponte* and grant summary judgment thereon risks depriving the court the benefit of advocacy on the issue, and depriving the parties of the opportunity to be heard"). We could not do so, as this would cause us to affirm on grounds that are not "supported by the record." ***Cassel-Hess***, 44 A.3d at 85.

Shamis v. Moon, 81 A.3d 962, 970 (Pa. Super. 2013). Instantly, we observe that Clarks relied on the Privacy Policy in support of its summary judgment motion, and made substantially similar arguments before the trial court as it makes on appeal. ***See*** MSJ, 7/15/25, at 14-17 (arguing Appellant consented to any interception based upon the Privacy Policy, which Clarks contends is similar to the privacy policy that warranted summary judgment in ***Popa III***); ***see also*** Appellant's Opposition to Clarks' MSJ, 8/22/25, at 21-24 (arguing Clarks failed to demonstrate Appellant's consent based upon the Privacy Policy and disputing ***Popa III***'s rationale). As the Privacy Policy was fully litigated before the trial court as a potential basis for summary judgment, we may consider it.

Initially, we note our agreement with the ***Popa III*** court that a reasonably prudent person has a lower expectation of privacy on the Internet, particularly with respect to the kind of non-sensitive data involved here.[11] ***Id.*** at 603. Reasonable Internet users "understand that what we do on the Internet is not completely private," but that "our data [is] going somewhere, … feeding an entire system of trackers, cookies, and algorithms designed to capture and monetize the information we generate." ***Id.*** at 602 (quoting ***In re Nickelodeon***, 827 F.3d at 266). Such practices are "commonly, if not ubiquitously, implicated in the use of a website," ***id.*** at 603, and the involvement of third parties in these practices is similarly common, if not ubiquitous. ***See id.*** at 600 (noting that "neither party's experts were able to identify a single website that does not use third-party resources"). Further, websites commonly disclose these practices in privacy policies posted on the website. ***See id.*** at 607.

While people rarely "think about" it, reasonable Internet users understand that when they "browse the Internet, … the data-collecting infrastructure of the digital world hums along quietly in the background." ***Id.***

---

[11] We agree with Appellant that WESCA is content-neutral, and a violation does not require that the contents of the intercepted communication be sensitive or private. ***See*** 18 Pa.C.S.A. § 5702 (defining, *inter alia*, "intercept" and "electronic communications"); ***see also*** Appellant's Brief at 41 (citing ***Bartnicki***, 532 U.S. at 526). Nevertheless, we consider the non-sensitive and, indeed, innocuous nature of the data at issue here to be relevant to the reasonable person standard.

at 602 (quoting ***In re Nickelodeon***, 827 F.3d at 266). Though "the nature of the Internet does not confer blanket implied consent to interception under WESCA," its nature is relevant to the reasonable person standard. ***Id.*** at 603. In other words, it is not reasonable for users to blithely assume they are browsing some idealized version of the Internet which does not, in fact, exist. Rather, "when determining whether a reasonable person can be deemed to consent to an interception under WESCA," courts "must be mindful of the reality of Internet communication…." ***Id.***

We further agree with the ***Popa III*** court that, under the reasonable person standard, a website's privacy policy may "convey [implied] consent to an interception" if it "disclose[s] the nature of the interception to a reasonable reader" and is "reasonably conspicuous" on the webpage. ***Id.*** at 603, 606.

Instantly, the Clarks website's Privacy Policy outlined to visitors "(i) what information we collect directly from you [(*i.e.*, the user)], and (ii) information we collect indirectly from you (primarily through cookies and web applications)"; and explained "how this information is handled, … the steps we take to ensure that it remains protected," and "where you may provide such information and how it is used." MSJ, 7/15/25, Exhibit F (Privacy Policy).

Under the heading "Information We Collect Indirectly and How We Use It," the Privacy Policy stated as follows:

> Cookies
>
> **Clarks uses cookies <u>and other technologies</u>** for digital remarketing and interest-based advertising purposes and to

better understand the needs and wants of our customers. Cookies are small data text files which are automatically transferred from our Site to your device or computer's hard drive for identification purposes. Cookies allow us to recognize your web browser every time you visit, so that we can personalize your experience and identify the areas of our Site which are most relevant to you.

Clarks also uses cookies to collect aggregate data about our customer base. Through the use of cookies, **we are able to track which parts of our Site are most popular, where our visitors are going, and how much time they spend there**. Such information helps us to provide you with improved services and a better overall site experience.

Clarks, together with a number of our third party partners, uses cookies to enhance the individual customer experience by doing such things as personalizing your on-site experience and tailoring marketing messages to you.

….

If you would prefer not to accept cookies from our Site, you can modify your browser preferences to refuse them. In order to do so, please refer to your browser's "help" section. Please keep in mind that rejecting or removing cookies could affect the availability and functionality of our services. **Please also note that your browser settings may not permit you to control the technologies utilized by third party companies**.

"Click Stream Data" and IP Address

In addition to using cookies, we also gather non-personally identifiable "click stream" data and store it in our website log files. **"Click stream" data records your Internet Protocol (IP) address, browser type, Internet Service Provider (ISP), previously visited web pages, and domain name**. We use this data to improve the content of our Site and to understand the demographics of our customer base.

Like most websites, our Site may incorporate technology such as "pixel tags" or "web beacons" that allow us to track the actions of users of our Site. Pixel tags or web beacons are tracking devices on websites or in e-mails that tell us when you have displayed that page or opened that email. This information is used to send you marketing and other

communications, including information about our products and promotions, that we think might interest you.

We also work with <u>third parties</u> who use click stream data to match your IP address against their customer information database. In these instances, you may receive direct mail from Clarks, without providing your home address directly to us. To opt out of these mailings, please click here to contact us.

Third parties and Your Information

Clarks works with reputable <u>third parties</u> who perform services on our behalf, some of whom require access to your personal information in order to properly assist us. For example, we may use third parties to host our Site, authorize and process credit card transactions, manage our gift card program, and administer tax calculations. We also work with **third parties** to whom we may disclose your personal information that have enterprise marketing platforms that provide such functions as data management, analytics and reporting on behavioral data, marketing campaigns, direct-mail services, and technology services that utilize third party customer data and match it against your personal information.

While on our Site, third parties with whom we work may place cookies on your browsers for purposes of tracking consumer behavior, and sending you targeted online and offline **advertising** including direct mail related to Clarks' products. When Clarks allows these **third parties** access to your personal information, we require that they handle your information with confidentiality and care, and use it solely for the business purpose for which it was intended. Clarks carefully selects business partners who exhibit our same high level of commitment to protecting your personal privacy.

Id. (emphasis added).

Finally, under the heading "Consent," the Privacy Policy stated that

[b]y using any of our Sites you signify that you agree to both the terms of this Privacy Policy and our stated Terms and Conditions. If you do not accept the terms of this Privacy Policy and/or our Terms and Conditions, please exit our Site and refrain from providing your personal information to us.

Id.

Our review of the Privacy Policy confirms that it adequately "disclose[s] the nature of the interception to a reasonable reader." ***Popa III***, 772 F. Supp. 3d at 603. The Privacy Policy explained that Clarks and its third-party partners used "cookies and other technologies," some of which functioned as "tracking devices on [the] website," with which Clarks and third parties could, *inter alia*, "track the actions of users of" the website and "record[]" a variety of information, including the user's IP address. Privacy Policy. Importantly, we observe that the Privacy Policy is rife with references to the involvement of third parties in these practices.

Appellant emphasizes she does not complain that Clarks itself tracked her information, but rather identifies, as the WESCA violation, the involvement of an "unknown third party (Content Square)," whom she characterizes as an "undisclosed eavesdropper[]." Appellant's Brief at 39, 44. However, the Privacy Policy amply disclosed that third parties would acquire the content of users' communications with the Clarks website. We conclude that reasonable readers of the Privacy Policy would know that the content of their

communications with the Clarks website would be intercepted by third parties.[12]

We acknowledge that the record, viewed in the light most favorable to Appellant, shows that she did not see the Privacy Policy and did not have actual knowledge of its disclosures. ***See*** Appellant's Deposition Transcript at 73. However, we reiterate that

---

[12] The Privacy Policy additionally indicated that it "applies only to the information collected by www.clarksusa.com." Privacy Policy. In his report, Appellant's expert, Mr. Strebe, opined that

> [f]rom a technical standpoint, the data collection by Content Square is not collected by www.clarksusa.com, it is collected by c.contentsquare.net. It is my opinion that a Privacy Policy that is applicable only to the information collected by www.clarksusa.com would not apply to the information collected by Content Square's tracking code, which is the relevant data in this case.

Appellant's Response to MSJ, 8/22/25, Exhibit C (Strebe Report) ¶ 71. We reject Mr. Strebe's legal interpretation of the Privacy Policy, as the technical distinction he purports to draw would not be appreciable by an average Internet user, but rather would be understood only by an advanced user who, like Mr. Strebe, had actual knowledge of the technology at play. ***See*** Appellant's Brief at 34 (arguing "the only way for a browser user to know that Content Square is receiving any transmissions during the browser session is with the use of advanced developer tools"). We agree with ***Popa III*** that "compliance with WESCA does not require that the [p]rivacy [p]olicy reveal granular details about the identity of the 'third parties' or the specific type of cookies used on the … website to confer information needed to establish consent." ***Popa III***, 772 F. Supp. 3d at 604 n.4. "Rather, WESCA focuses on the *event* of an interception rather than the specific details thereof." ***Id.*** (emphasis added).

Mr. Strebe further opined that the Privacy Policy was inapposite because "[e]ven if a user went straight from the homepage to a privacy policy page, … the user's request … for the privacy policy URL" would be captured. Strebe Report ¶ 82. The ***Popa III*** court rejected an identical argument, and we agree with and adopt its analysis. ***Popa III***, 772 F. Supp. 3d at 608 n.6.

> the phrase "actual knowledge" does not appear in the statutory language of [WESCA's] mutual consent exception…. Rather, our case law illustrates that "prior consent" can be demonstrated when the person being recorded "knew **or should have known**, that the conversation was being recorded." ***Diego***, 119 A.3d at 377. This standard is one of a reasonable person, and not proof of the subjective knowledge of the person being recorded….

Byrd, 235 A.3d at 319 (emphasis added). "As in ***Byrd***, the question" before us is not whether Appellant "had actual knowledge, but rather, whether a reasonable person can be found to have provided implied consent to the alleged interception by her actions." ***Popa III***, 772 F. Supp. 3d at 604. "To make this determination," we "must consider whether a reasonable person in [Appellant's] circumstance could be charged with implicit knowledge of the disclosures in the [Privacy Policy]. This turns on the visibility and accessibility of the [Privacy Policy] to an ordinary user." ***Id.***

Like the privacy policy at issue in ***Popa III***, Clarks' Privacy Policy is a browsewrap agreement, which "does not require the user to manifest assent to the terms and conditions expressly," but provides that a "party instead gives his assent simply by using the website." ***Id.*** at 604-05 (quoting ***Nguyen***, 763 F.3d at 1176).

In her reply brief, Appellant relies on ***Duffy v. Tatum***, 354 A.3d 14 (Pa. Super. 2026), in which this Court held "that the constitutional right to a jury trial should be afforded the greatest protection under the courts of this Commonwealth," and that "a strict burden of proof is necessary to demonstrate a person's unambiguous manifestation of assent to arbitration."

Id. at 25; ***see*** Appellant's Reply Brief at 27-28. The ***Duffy*** Court determined the plaintiff did not manifest assent to an arbitration agreement when he registered for services on the defendant's website, reasoning as follows:

> Duffy never clicked on the hyperlink providing the terms of service[, which contained the arbitration agreement]. [The defendant's] website and application screen does not explicitly state that the consumer is waiving their right to a jury trial when they agree to the terms of service. Duffy was able to complete his registration process without being fully informed of the waiver of his right to a jury trial. The hyperlink that opens the terms of service hides the arbitration agreement within the middle of the document and does not place it in prominently in the document. Further, the arbitration provision never defines arbitration and does not state explicitly that a user is waiving his right to trial by jury. Therefore, it is clear Duffy was never informed in an explicit and upfront manner that he was waiving his constitutional right to seek damages through a jury trial.

Duffy, 354 A.3d at 25.

Appellant maintains that "the inquiry here," as in ***Duffy***, "must … focus on whether [Appellant] took any action that manifested [her] assent to be bound by the terms and conditions on [Clarks'] website." Appellant's Reply Brief at 28 (quoting ***Duffy***, 354 A.3d at 23). However, ***Duffy***'s utility is limited, as the issue before us is not one of constitutional dimension. Appellant did not waive an important constitutional right; rather, the contents of her innocuous communications with a retail website were acquired by a "reputable third part[y] … perform[ing] services on [the retailer's] behalf." Privacy Policy. Indeed, the alleged infringement at issue here is of such low stakes that the Third Circuit has determined that, even if it technically constitutes a WESCA violation, it is not a legally cognizable injury sufficient to

invoke Article III jurisdiction. ***See GameStop***, 148 F.4th at 158-63; ***Popa IV***, 2026 WL 837280, at *1 (non-precedential opinion). We therefore decline to impose a heightened burden of proof requiring a demonstration of a person's unambiguous manifestation of assent.

We observe that the ***Duffy*** Court reached its conclusion only after considering "what a reasonable person in [the plaintiff's] position would understand by using [the defendant's] website." ***Duffy***, 354 at 23. Reasonable people undoubtedly have different expectations with respect to the waiver of important constitutional rights than they have regarding the acquisition of their non-sensitive data by the Internet's nearly-ubiquitous "data-collecting infrastructure." ***In re Nickelodeon***, 827 F.3d at 266. A reasonable person's implied consent to the latter may be demonstrated by something less than an affirmative action unambiguously manifesting assent. In accordance with our above observations regarding the nature of the Internet, we determine that a website's browsewrap privacy policy, if reasonably conspicuous, may be sufficient to demonstrate that a reasonable user should know about the data-collection practices disclosed in the policy, thereby conferring implied consent under WESCA section 5704(4). ***See Popa II***, 52 F.4th at 132 ("Prior consent, including implied consent, 'can be demonstrated when the person being recorded knew or should have known[] that the conversation was being recorded.'" (quoting ***Byrd***, 235 A.3d at 319)); ***Popa III***, 772 F. Supp. 3d at 606 (holding the browsewrap "Privacy

Statement on Harriet Carter's website was reasonably conspicuous on the webpage so as to charge Popa with constructive notice that continued use constituted acceptance of the agreement." (citations, quotation marks, and brackets omitted)).

We agree with the ***Popa III*** court's analysis regarding the circumstances under which a privacy policy may be considered reasonably conspicuous. ***Id.*** at 604-08. A privacy policy is not likely to be deemed conspicuous if it is linked in "obscure sections of a webpage that users are unlikely to see." ***Id.*** at 605 (quoting ***James***, 852 F.3d at 267). Conversely, "[w]here the manner of posting a privacy policy was consistent with common industry practice, and the appearance of the language was visible and not hidden in an obscure place on the website, a court should [be] … hesitant to find that the posted terms were incapable of conveying constructive notice." ***Id.*** at 607. The privacy policy upon which the ***Popa III*** court based its summary judgment grant was linked in the website's footer, which the plaintiff's expert testified was a common industry practice. ***Id.***

Instantly, Clarks represents that its own Privacy Policy's hyperlink was similarly posted in the website's footer, "conspicuous[ly]" located at the center and bottom of the webpage, such that Appellant, "or any other user, could have easily seen it and understood its contents." Clarks' Brief at 27 n.9. (quoting ***Popa III***, 772 F. Supp. 3d at 606-07).

Appellant counters that Clarks' representation regarding the location of the Privacy Policy is unsupported by record evidence. Appellant's Reply Brief at 26. Appellant maintains that "Clarks did not submit evidence to the trial court demonstrating where the Privacy Policy resided on its website or how a typical visitor to the website would have been apprised of its existence." ***Id.***; ***see also*** Appellant's Opposition to Clarks' MSJ, 8/22/25, at 21 n.14 (arguing Clarks cited no record evidence supporting its representation, in its brief in support of its MSJ, that the Privacy Policy was located at the center and bottom of the webpage).

Our review discloses that Clarks' representation regarding the location of the Privacy Policy on its website is not supported by the record before us. We further observe that Clarks' representation is unaccompanied by a citation to the record. ***See*** Clarks' Brief at 27 n.9; ***see also*** Clarks' Brief in Support of MSJ, 7/15/25, at 16 n.9. The Privacy Policy itself is contained in the record, ***see*** MSJ, 7/15/25, Exhibit F (Privacy Policy), and it is apparently undisputed that the Privacy Policy existed on Clarks' website during the relevant time period. Appellant's expert report suggests, without stating outright, that the Privacy Policy could be accessed directly from the website's homepage. ***See*** Strebe Report ¶ 82. But the record is seemingly devoid of specific evidence regarding the Privacy Policy's location and visibility on the website. We lack, for example, a screenshot of the website depicting the link to the Privacy

Policy, similar to that which the ***Popa III*** court relied upon in reaching its conclusion. ***See Popa III***, 772 F. Supp. 3d at 607.

We reiterate that we must "view the record in the light most favorable to the nonmoving party" and resolve "all doubts as to the existence of a genuine issue of material fact … against the moving party." ***Huggins***, 359 A.3d at 468. The instant record contains insufficient information to support a determination that the Privacy Policy was reasonably conspicuous on the Clarks website, such that Appellant's consent to the data-collection practices it disclosed may be implied under WESCA section 5704(4). We therefore cannot determine that Clarks met its burden, as the moving party, "to demonstrate the absence of any issue of material fact" with respect to Appellant's consent. ***Edwards v. Norfolk S. Ry. Co.***, 337 A.3d 525, 528 (Pa. Super. 2025) (*en banc*) (citation omitted). Thus, for this reason, we cannot affirm the grant of summary judgment in Clarks' favor.

Accordingly, we vacate the order granting summary judgment and remand for further consideration, without prejudice to Clarks again moving for summary judgment. In light of our clarification of the applicable law, the parties may supplement the record and, if the trial court deems appropriate, engage in additional discovery.

Based on our disposition of Appellant's first two issues, we need not dwell upon her third issue.[13]

---

[13] Appellant's third issue challenges the import of the trial court's statement that she "has not produced evidence that her [interaction with the Clarks website] was actually recorded by Session Replay," but instead relied on evidence of other forms of data tracking. Trial Court Opinion, 12/5/25, at 10; ***see also*** Appellant's Brief at 13, 26-31; Appellant's Reply Brief at 11-19. "Session replay code is a script of computer code that enables a company to track how internet users browse and interact with its website. It captures a user's mouse movements, clicks, keystrokes, and more. A session replay code provider then aggregates the data into a video for the company reenacting the user's visit." ***GameStop***, 148 F.4th at 156 (footnote omitted).

Appellant's complaint alleged that Clarks procured third-party vendors to use session replay code on its website, ***see*** Complaint, 2/14/23, ¶ 1, but Appellant now concedes the evidence shows "that Clarks only paid Content Square to create Session Replay videos for 1% of the total visits to Clarks' website." Appellant's Reply Brief at 14. Appellant argues her "evidence shows that Content Square was intercepting 100% of the communications that visitors made with Clarks' website. The amount of those visits that were later converted into full session replay videos for Clarks is immaterial," as the initial interception constitutes a WESCA violation. ***Id.*** Clarks contends Appellant's complaint was based exclusively on "Session Replay Code," and argues her reliance on evidence of data tracking via other means constitutes a new theory, outside the bounds of the complaint. Clarks' Brief at 3 n.1; ***see also id.*** at 31-38. Appellant maintains her theory has never changed, and argues her complaint defined "Session Replay Code" so broadly as to encompass the type of interception her evidence shows, regardless of whether her own data was aggregated into a session replay video. Appellant's Brief at 7 n.1 (citing Complaint, 2/14/23, ¶ 1).

We observe that the trial court's statement on the lack of session replay evidence did not form the basis of its ruling; rather, as we noted above, its determination that Appellant consented to the tracking presupposes that an interception occurred. ***See*** Trial Court Opinion, 12/5/25, at 10-11. We have also concluded there is evidence of an interception. Our review of the complaint confirms that its allegations fairly encompass the type of data tracking shown by the evidence, regardless of whether that tracking meets a strict definition of "session replay code." ***See generally*** Complaint, 2/14/23.
(Footnote Continued Next Page)

Order vacated. Case remanded for further proceedings consistent with this opinion. Jurisdiction relinquished.

Judgment Entered.

Benjamin D. Kohler

Benjamin D. Kohler, Esq.
Prothonotary

DATE: 10/23/2026

In short, the lack of session replay evidence neither formed the basis of the trial court's summary judgment grant, nor does it serve as an alternative ground for affirmance.