8-16-2022

Ashley Popa v. Harriet Carter Gifts Inc.

PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 21-2203

ASHLEY POPA,
individually and on behalf of all others similarly situated,

Appellant

v.

HARRIET CARTER GIFTS, INC., a Pennsylvania corporation; NAVISTONE, INC., a Delaware corporation

---

Appeal from the United States District Court
for the Western District of Pennsylvania
(D.C. Civil Action No. 2-19-cv-00450)
District Judge: Honorable William S. Stickman, IV

Argued on June 8, 2022

Before: CHAGARES, Chief Judge, AMBRO, and
FUENTES, Circuit Judges

(Opinion Filed August 16, 2022)

Jamisen A. Etzel
Kelly K. Iverson
Gary F. Lynch **(Argued)**
Elizabeth Pollock-Avery
Lynch Carpenter
1133 Penn Avenue
5th Floor
Pittsburgh, PA 15222

Counsel for Appellants

Sarah A. Ballard
Paul G. Karlsgodt **(Argued)**
Baker & Hostetler
1801 California Street
Suite 4400
Denver, CO 80202

Carrie H. Dettmer Slye
Baker & Hostetler
312 Walnut Street
Suite 3200
Cincinnati, OH 45202

Counsel for Appellee Harriet Carter Gifts, Inc.

David W. Bertoni, I **(Argued)**
Eamonn R. C. Hart
David Swetnam-Burland
Brann & Isaacson
184 Main Street
4th Floor
P. O. Box 3070

Lewiston, ME 04240

Devin J. Chwastyk
Rachel R. Hadrick
McNees, Wallace & Nurick
100 Pine Street
P. O. Box 1166
Harrisburg, PA 17101

Counsel for Appellee NaviStone, Inc.

OPINION OF THE COURT

AMBRO, Circuit Judge

This case began with a quest for pet stairs. Searching for that item, Ashley Popa browsed the website of Harriet Carter Gifts, added a set of stairs to her cart, but then left the website without making a purchase. That might have been the end of it. But she later discovered that, unbeknownst to her as she was browsing the website, a third-party marketing service Harriet Carter was using, NaviStone, tracked her activities across the site. This, Popa believed, violated Pennsylvania's anti-wiretapping law, and she sued both entities (collectively, the "Defendants") in a Pennsylvania court (though they later removed the case to federal court).

Pennsylvania's Wiretapping and Electronic Surveillance Control Act ("WESCA" or "Act"), 18 Pa. C.S. § 5701 *et seq.*, prohibits the interception of wire, electronic, or

oral communications, which means it is unlawful to acquire those communications using a device. The District Court granted summary judgment for NaviStone and Harriet Carter. It held NaviStone could not have "intercepted" Popa's communications, because it was a "party" to the electronic conversation. Alternatively, it ruled that if any interception did occur, it happened outside Pennsylvania's borders; thus the Act did not apply. As we read Pennsylvania law differently on both holdings, we vacate the Court's grant of summary judgment and remand.

I. Background

In 2018, Ashley Popa used her iPhone to view Harriet Carter Gifts' website. A pop-up window asked for her email address, which she provided. She searched for pet stairs, added a set to her cart, and began (but never completed) the checkout process.

There was more to that online interaction than met the eye. As Popa clicked links, used the search function, and tabbed through form fields on the website, her browser simultaneously communicated with two entities: Harriet Carter (this Popa obviously knew) and a third-party marketing service, NaviStone, that it was using (this Popa did not know). Her communications with Harriet Carter told the website what to display on her screen and what to place in her cart. The messages to NaviStone alerted it to how Popa was interacting with the website (which pages she visited, when she filled in an email address, when she added an item to her cart, and so on).

The testimony and evidence are technical about how these communications were sent, but the important points for

our purposes are not. When Popa—or any other user at that time—loaded the Harriet Carter website, her browser sent a "GET request" to the Harriet Carter server. The server responded by sending HTML code to the user's browser. The browser interpreted this code to allow the website to appear on the user's screen. Harriet Carter's HTML code also included some JavaScript that told the user's browser to send *another* GET request to NaviStone's server in Virginia. That server responded by sending its own "OneTag" code to Popa's browser. Once the browser loaded the OneTag code, two things happened. First, the code placed cookies on the user's browser so that her activity on the webpage had an associated visitor ID. Second, the code told the user's browser to begin sending information to NaviStone as she navigated through the website, such as communicating that the user had clicked the "add to cart" button or tabbed out of a form field. NaviStone could later use this information to identify which of Harriet Carter's customers may be receptive to promotional mailings.

In 2019, Popa sued Harriet Carter and NaviStone over their use of the OneTag software. She brought two counts: a claim for violation of the WESCA and a common law claim for invasion of privacy. The District Court dismissed the common law claim but allowed the WESCA claim to go to summary judgment. As noted, on summary judgment the Court ruled for the Defendants. Popa now appeals.[1]

[1] The District Court exercised diversity jurisdiction under 28 U.S.C. § 1332(d)(2). Popa appeals the Court's grant of summary judgment, so we have jurisdiction under 28 U.S.C. § 1291.

II. Standard of Review

We give a fresh (that is, *de novo*) review to the District Court's grant of summary judgment, viewing the facts and making all reasonable inferences in the non-movant's favor. *TitleMax of Del., Inc. v. Weissmann*, 24 F.4th 230, 236 n.3 (3d Cir. 2022). Summary judgment is appropriate if "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a).

When asked to interpret provisions of Pennsylvania law, "the decisions of the Pennsylvania Supreme Court are the authoritative source." *Spence v. ESAB Grp., Inc.*, 623 F.3d 212, 216 (3d Cir. 2010). If there is no controlling decision, our task is to predict how that Court would rule on an issue. *Id.* That may be informed by "decisions of state intermediate appellate courts, of federal courts interpreting that state's law, [] of other state supreme courts that have addressed the issue," and other sources "tending convincingly to show how the highest court in the state would decide the issue at hand." *Id.* at 216–17 (internal quotation marks omitted).

III. Discussion

The WESCA offers a private civil cause of action to "[a]ny person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of [that statute]" against "any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication." 18 Pa. C.S. § 5725(a). In other words, it prohibits intercepting communications and allows someone whose communications have been intercepted to sue the offender. It also operates in conjunction with and as a supplement to the Federal Wiretap Act, 18 U.S.C. § 2510 *et*

seq., which provides uniform minimum protections for wire, electronic, or oral communications. The States—like Pennsylvania—may "grant greater, but not lesser, protection than that available under federal law," as the WESCA does. *Commonwealth v. Spangler*, 809 A.2d 234, 237 (Pa. 2002).

Popa, here proceeding only under Pennsylvania's Act, contends that NaviStone violated that statute by intercepting her communications with Harriet Carter Gifts' website. Harriet Carter, in turn, also violated the Act, she asserts, by "procur[ing] any other person [*i.e.*, NaviStone] to intercept" her communications. 18 Pa. C.S. § 5725. The Defendants, though, argue that under Pennsylvania law no interception can occur when the communications are received by a direct party, which they say NaviStone was. Plus they make two alternative arguments: first, even if they did intercept Popa's communications, the WESCA does not reach their conduct because any interception occurred outside the Commonwealth; second, they had Popa's implied consent to intercept. We address each argument in turn.

A.

NaviStone and Harriet Carter are liable to Popa only if NaviStone "intercepted" Popa's communications. 18 Pa. C.S. § 5725(a). So the first question is, what does it mean to "intercept"?

This is a term of art in the wiretap context. Though in normal conversation "intercept" means to "stop, seize, or interrupt in progress"—such as when a safety jumps between the quarterback and wide receiver to break up a pass—the WESCA gives the word a "broader connotation than the ordinary meaning." *In re Google Inc. Cookie Placement*

Consumer Priv. Litig., 806 F.3d 125, 144 n.80 (3d Cir. 2015) (interpreting the identical portion of the Federal Wiretap Act's definition of "intercept") (internal quotation marks omitted). Under Pennsylvania's Act, it is just 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."[2] 18 Pa. C.S. § 5702.

The WESCA's use of "intercept" thus reduces to acquiring certain communications using a device. And based on just that definition, anyone could "intercept" communications, including people who "acquire" a text message or chat sent directly to them. The Defendants, though, argue that Pennsylvania courts have added a gloss to the Act's statutory definition, making it so that no interception occurs when a direct recipient is the one acquiring the communications. They also claim that because NaviStone was a direct party to Popa's communications, they are free from all liability.

Had we considered this case a decade ago, we might agree. As the Defendants point out, for years Pennsylvania courts routinely determined there is no interception under the WESCA when the alleged "interceptor" was the intended recipient of the information. Two Pennsylvania cases illustrate this.

In the first, *Commonwealth v. Proetto*, a defendant was convicted of criminal solicitation (among other things) based on his internet chatroom messages with a 15-year-old girl. 771 A.2d 823, 826–27 (Pa. Super. Ct. 2001). E.E., the victim,

[2] The Federal Wiretap Act's definition uses identical language for "intercept." 18 U.S.C. § 2510(4).

saved her online conversations with the defendant and handed them over to the police. *Id.* at 826. Later, when a detective entered the chatroom impersonating another 15-year-old girl, he logged messages the defendant sent "her" asking for a nude video in exchange for nude photos of himself. *Id.* at 827. The defendant later tried to suppress the evidence of his chat logs, claiming the police obtained them in violation of the WESCA. *Id.*

The Pennsylvania Superior Court held that statute was not in play because the communications were not "intercepted." *Id.* at 828–29, 831–32. Particularly, the detective's use of the chatroom was not an "interception" because he was the "intended recipient of [the defendant's] communications," even if he misrepresented his true identity. *Id.* at 831. Thus when "a party receives information from a communication as a result of being a direct party to the communication, there is no interception." *Id.*

In a second case, *Commonwealth v. Cruttenden,* the Pennsylvania Supreme Court reaffirmed *Proetto*'s holding: when something is communicated to a direct recipient, there is "no eavesdropping or listening in," so "no interception [could take] place." 58 A.3d 95, 100 (Pa. 2012). In that case, an officer used the phone of the defendant's accomplice to text the defendant about a drug deal. *Id.* at 96. Posing as the accomplice, the officer answered several questions from the defendant to confirm his identity before the defendant began to confide in him. *Id.* When those text messages were later used at trial, the defendant tried to suppress them as violations of the WESCA. *Id.* at 97.

The Pennsylvania Supreme Court, relying at length on *Proetto*, held that there was no WESCA violation because the

officer was the "intended recipient" of the communication. *Id.* at 100. "That a police officer does not identify him- or herself, or misrepresents his or her identity, does not change the fact that he or she is a direct party to the conversation, and by virtue of being a direct party to the conversation, is deemed the intended recipient of the conversation under whatever identity the officer has set forth." *Id.*

If these cases stood alone, their expansive language would, as the Defendants argue, strongly suggest the Pennsylvania courts have carved out direct recipients from the WESCA's reach. But they aren't the last word on the issue. In 2012, a new set of the Pennsylvania General Assembly's amendments to the WESCA went into effect, including an expanded definition of "intercept." That definition now reads (with the added language underlined):

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

> 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.

18 Pa. C.S. § 5702.

The third sentence is a key change. In adding it, the specific facts and holdings of *Proetto* and *Cruttenden*—exempting a law enforcement officer from liability for acquiring communications when he is an "intended recipient" or is posing as one—are now explicitly included as a carve-out in the definition of "intercept." *Id.* But this also limits the expansive reach of those cases.

The "inclusion of a specific matter in a statute implies the exclusion of other matters" under the *expressio unius est exclusio alterius* (the expression of one thing is the exclusion of the other) canon of statutory interpretation. *Atcovitz v. Gulph Mills Tennis Club, Inc.*, 812 A.2d 1218, 1223 (Pa. 2002); *see also Andrus v. Glover Constr. Co.*, 446 U.S. 608, 616–17 (1980) ("Where Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied, in the absence of evidence of a contrary legislative intent."). Thus inclusion of one exception implies the deliberate exclusion of another. Here the Pennsylvania legislature decided to codify a specific, narrow intended-recipient exemption for law enforcement, limiting

Proetto and *Cruttenden* to their facts. This implies it chose to reject the broader implications of those cases.

Indeed, it had the opportunity to adopt the expansive language from those opinions. And it had a prototype for a direct-party exception in the Federal Wiretap Act. *See* 18 U.S.C. § 2511(2)(d) ("It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication *where such person is a party to the communication* or where one of the parties to the communication has given prior consent to such interception." (emphasis added)). Still it codified only a law-enforcement exception, thus limiting any direct-party exception to that context.[3] And even that exception was narrower than the *Proetto* exception or that of the Federal Wiretap Act. The text shows that, even for law enforcement, being a direct party is

[3] The Defendants argue we should not read the 2012 amendment as a rejection of a broad direct-party exception. They believe the Pennsylvania legislature enacted the amendment "to address a narrow issue relating to police activity arising out of the *Cruttenden* case, and specifically to undo a lower court decision in that case" that seemed to undermine *Proetto*. Defs.' Suppl. Br. at 1. Though we agree the legislative history cited by the Defendants suggests the Pennsylvania legislature enacted the 2012 amendment to preserve the *Proetto* exception, we disagree with their conclusion that this means the legislature preserved the broader exception in those cases. When it codified *Proetto*, it did not choose to codify the broader language from that opinion, as it could have. Had it truly wished to preserve everything *Proetto* implied, it could have codified a direct-party exception like the one in the Federal Wiretap Act.

not enough to exempt officers from liability: they must also have the prior approval of a supervising official to make their actions lawful.

Indeed, the broader exception the Defendants ask us to read into the statute conflicts with the rest of the Act. It excepts a range of conduct from the general bar against wiretapping. *See* 18 Pa. C.S. § 5704. One exception makes it lawful for "[a] person, to intercept a wire, electronic or oral communication, where *all parties* to the communication have given prior consent to such interception." *Id.* § 5704(4) (emphasis added). If, as the Defendants argue, 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 disappears.[4]

Under Pennsylvania law, then, there is no direct-party exception to liability under the WESCA (save for law enforcement under specific conditions).[5] So NaviStone and

---

[4] To give another example, the WESCA creates an exception for an interception by a law enforcement officer where the officer is a party to the communication and the other party is either holding a hostage or has barricaded himself to avoid apprehension and that party either may resist with the use of weapons or is threatening harm to himself or others. *See* 18 Pa. C.S. § 5704(12). This exception shows it is simply not enough for the person making the interception to be a direct party to the communication; that is only the first of several conditions necessary to make the interception lawful.

[5] We thus need not consider Popa's argument that NaviStone was *not* a direct party, as NaviStone could remain liable whether a direct party or not.

Harriet Carter cannot avoid liability merely by showing that Popa directly communicated with NaviStone's servers.[6]

B.

This leads to our next question: when NaviStone intercepted Popa's electronic communications, where did that interception occur? The answer is important because Pennsylvania courts have declined to extend the WESCA to cover conduct occurring wholly outside the Commonwealth—at least in the context of recording telephone conversations. *Larrison v. Larrison*, 750 A.2d 895, 898 (Pa. Super. Ct. 2000). When a person in New York, for example, tape records a phone call with someone in Pennsylvania, the WESCA does not apply because the Commonwealth has "no power to control the activities that occur within a sister state." *Id.*

There are two possible "intercept" points here. One, which the District Court recognized and the Defendants now

[6] This of course contrasts with our decisions involving the *Federal* Wiretap Act in *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125 (3d Cir. 2015), and *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262 (3d Cir. 2016). There we decided the defendants were not liable under the Federal Wiretap Act because the users' browsers sent GET requests directly to the defendants, making them "parties" to the communication. *In re Google*, 806 F.3d at 142–43; *In re Nickelodeon*, 827 F.3d at 274. As we already mentioned, the Federal Wiretap Act—unlike the WESCA—has an explicit direct-party exemption. *See* 18 U.S.C. § 2511(2)(d). So we reached a different conclusion in those cases by applying that exemption. *In re Google*, 806 F.3d at 142–43; *In re Nickelodeon*, 827 F.3d at 274.

argue for, is when Popa's electronic communications reached their final destination at NaviStone's servers in Virginia. If this is the sole point of interception, then we would need to conduct a choice-of-law analysis to determine whether the WESCA should reach this conduct. *See id.* The other, pushed by Popa, is when the electronic communications were sent from Popa's browser to NaviStone without her knowledge. She asserts this occurred within Pennsylvania's borders. If so, under her theory, Pennsylvania law should apply.

The WESCA does not demarcate where an interception occurs. Yet we know from the statute's definition that an interception involves 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. § 5702. And while the statute does not further define "acquisition," we can apply the word's "common and approved usage." 1 Pa. C.S. § 1903(a). "Acquisition" means "the act of acquiring." Webster's New Collegiate Dictionary 11 (1977). And "acquire," in turn, means "to come into possession or control of," *id.*, or to "gain [or] obtain," The Oxford Dictionary of English Etymology 9 (1966). The result is that an interception occurs where there is an act taken to gain possession of communications using a device.

Sometimes that place is obvious. Picture the days before wireless communication when police tapped a phone line by cutting the telephone wire that carried the conversation from one line to the other and adding a wire to the officer's own phone. There, cutting the wire and attaching another one is clearly an act taken to gain possession of the wire communication, and thus an intercept occurred where that wire was cut. This tracks the holdings of several federal courts of appeals that have interpreted the identical portion of the federal

definition of "intercept": when the contents of a communication are "captured or redirected in any way, an interception occurs at that time." *United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992); *see also, e.g.*, *United States v. Denman*, 100 F.3d 399, 403 (5th Cir. 1996). So, in the telephone wiretap context, the "jurisdiction in which the to-be-tapped telephone is located" is one certain place where an interception occurred, for that is where the communications are rerouted, whether the listener is in the state or not. *Rodriguez*, 968 F.2d at 136; *see also United States v. Luong*, 471 F.3d 1107, 1109 (9th Cir. 2006) ("The most reasonable interpretation of the statutory definition of interception is that [it] occurs where the tapped phone is located *and* where law enforcement officers first overhear the call." (emphasis in original)).

Electronic communications are similarly "intercepted" when software reroutes communications to an interceptor. Take the Sixth Circuit case, *Luis v. Zang*, 833 F.3d 619 (6th Cir. 2016). A jealous husband installed software, WebWatcher, on his wife's computer so he could monitor her online conversations. *Id.* at 623–24. Once installed, it would "automatically acquire[] and transmit[] communications" such as emails and chat messages to the software manufacturer, Awareness, at its servers in California. *Id.* at 633. A man with whom the wife was communicating sued Awareness after his online communications were directed to its servers. *Id.* at 624. Though Awareness tried to argue that the husband, not it, had intercepted the communications by later viewing them, the Sixth Circuit disagreed. *Id.* at 633. The "intercept of a communication," it said, "occur[red] at the point where WebWatcher—without any active input from the user—capture[d] the communication and reroute[d] it to Awareness's

own servers." *Id.* As with tapped phones, Awareness "'acquire[d]' the communications by *rerouting* them to servers that it owns and controls."[7] *Id.* (emphasis added).

So NaviStone intercepted Popa's communications at the point where it routed those communications to its own servers. And that was at Popa's browser, not where the signals were received at NaviStone's servers. The Defendants' own evidence details how NaviStone went about obtaining the communications. It provided JavaScript code to Harriet Carter to install on its website. This code would "begin[] to run when the website page, which includes the code, [was] fully rendered and loaded in the visitor's web browsing software." Appx. at 189. Then, when the user interacted with the website in specific ways (such as by adding an item to a cart or tabbing out of a form field), "the code *cause[d]* certain communications to be sent from the visitor's web browser directly to NaviStone." *Id.* at 188 (emphasis added); *see also id.* at 189–91 (detailing which communications triggered messages to NaviStone). Thus when the code—the rerouting

[7] That is not to say that an interception fails also to occur where the information is ultimately received by the "listener." Our Circuit has also adopted the "listening post" theory—at least for federal wiretaps—which holds that an interception can take place also where the contents of the communication are heard by law enforcement officers. *United States v. Jackson*, 849 F.3d 540, 551 (3d Cir. 2017). Whether this theory extends to the WESCA or electronic communications is another question for another day.

device at issue[8]—told Popa's browser to send communications to NaviStone and those electronic signals were routed to NaviStone's servers, an interception occurred.[9]

The problem, though, is we still don't know exactly where Popa's browser accessed the Harriet Carter website and

---

[8] The Defendants do not argue on appeal that the JavaScript on Harriet Carter's website is not a "device." We therefore assume for the purposes of this opinion that it is.

[9] The Defendants argue against this interpretation of the statute, invoking the constitutional-doubt canon. Specifically, they urge that "[a]pplying WESCA to NaviStone based on conduct that occurred wholly outside of Pennsylvania would have the 'practical effect' of regulating commerce occurring wholly outside Pennsylvania and would thus violate the Commerce Clause." Defs.' Br. at 44.

We decline to apply this canon for two reasons. First, before it "may be used, there must exist a doubt as to the meaning of the statute." *United States v. Grier*, 475 F.3d 556, 567 n.7 (3d Cir. 2007); *see also 1256 Hertel Ave. Assocs., LLC v. Calloway*, 761 F.3d 252, 261 (2d Cir. 2014) ("Application of the [constitutional-doubt] canon requires that the statute in question be genuinely susceptible to at least two interpretations . . . ."). And here there is no genuine doubt about the plain meaning of the statute. Second, we need not apply this canon when "a constitutional question, while lacking an obvious answer, does not lead a majority gravely to doubt that the statute is constitutional." *Almendarez-Torres v. United States*, 523 U.S. 224, 239 (1998). Though the Defendants raise interesting constitutional issues about the States' ability to regulate internet communications more generally, we do not have grave doubts as to the constitutionality of the WESCA.

where NaviStone's JavaScript began telling the browser to communicate with its servers. The parties seem to assume this occurred in Pennsylvania, but they point us to no source in the record confirming this point. We therefore leave it to the District Court to determine anew whether there is a genuine issue of material fact about where the interception occurred. While we do not resolve this question in this appeal, we do hold that the place of interception is the point at which the signals were routed to NaviStone's servers.[10]

C.

So does this mean websites can never use cookies or third-party marketing companies to analyze customer data? Though the Defendants try to convince us about the certainty of any number of "parade of horribles," the WESCA is not so unreasonable. It, like the Federal Wiretap Act, includes many exceptions from liability. One is the all-party consent exception, under which it is not unlawful for someone to "intercept a wire, electronic or oral communication, where all parties to the communication have given prior consent to such interception." 18 Pa. C.S. § 5704(4). Thus if someone consents to the interception of her communications with a

[10] We note that the Defendants' interpretation of the statute (that communications are only intercepted when received at the server) would also lead to absurd results. Under this theory, companies could capture the data of people in other states as long as they parked their servers in a state with weak privacy protections. That would significantly undermine the privacy protection that is at the core of the WESCA and would be inconsistent with the General Assembly's intent. *See Spangler*, 809 A.2d at 237 (discussing how the WESCA "emphasizes the protection of privacy").

website, the WESCA does not impose liability. Here the Defendants obviously consented to the interception. The question is whether Popa did as well.

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." *Commonwealth v. Byrd*, 235 A.3d 311, 319 (Pa. 2020). 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.[11]

These are arguments that should be addressed first by the District Court. We generally decline to resolve issues not

[11] Though a senior Harriet Carter employee attested in a declaration that the privacy policy was on the website during the relevant period, later in a deposition he said he could not provide the privacy policy as it existed in 2018.

decided by a district court, choosing instead to allow it to decide in the first instance. *Forestal Guarani S.A. v. Daros Int'l, Inc.*, 613 F.3d 395, 401 (3d Cir. 2010). And this is particularly appropriate here because there are unresolved disputes about the evidence supporting the Defendants' privacy policy arguments. *See* Doc. 97 (Popa objecting to portions of the declarations of Larry Kavanagh, Chris Ludwig, and Greg Humphreys, including challenging parts discussing the privacy policy); Appx. at 21 (denying as moot Popa's evidentiary objections). These objections will need to be resolved before determining whether the Defendants are entitled to summary judgment on the basis of Harriet Carter's privacy policy.

* * *

The WESCA "emphasizes the protection of privacy." *Spangler*, 809 A.2d at 237. Consistent with that emphasis, it applies when anyone intercepts communications—that is, takes an action to acquire them with a device. And it requires all parties—not just *a* party—to consent to that interception. As we part with the District Court's holding that NaviStone is exempt from liability because it was a direct party to Popa's communications and that interception only occurred at the site of NaviStone's servers in Virginia, we vacate the Court's order granting summary judgment and remand for further consideration.