RECOMMENDED FOR FULL-TEXT PUBLICATION
Pursuant to Sixth Circuit I.O.P. 32.1(b)

File Name: 16a0196pp.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

JAVIER LUIS,

Plaintiff-Appellant,

v.

JOSEPH ZANG et al.,

Defendants,

AWARENESS TECHNOLOGIES,

Defendant-Appellee.

No. 14-3601

Appeal from the United States District Court
for the Southern District of Ohio at Cincinnati.
No. 1:12-cv-00629—Susan J. Dlott, District Judge.

Argued: April 27, 2016

Decided and Filed: August 16, 2016

Before: MERRITT, BATCHELDER, and GILMAN, Circuit Judges.

COUNSEL

ARGUED: Clayton L. Wiggins, VANDERBILT APPELLATE LITIGATION CLINIC, Nashville, Tennessee, for Appellant. Bernard W. Wharton, MCCASLIN, IMBUS & MCCASLIN, Cincinnati, Ohio, for Appellee. **ON BRIEF:** Clayton L. Wiggins, Alistair E. Newbern, VANDERBILT APPELLATE LITIGATION CLINIC, Nashville, Tennessee, for Appellant. Bernard W. Wharton, MCCASLIN, IMBUS & MCCASLIN, Cincinnati, Ohio, for Appellee. Javier Luis, Tampa, Florida, pro se.

GILMAN, J., delivered the opinion of the court in which MERRITT, J., joined. BATCHELDER, J. (pp. 33–37), delivered a separate dissenting opinion.

OPINION

RONALD LEE GILMAN, Circuit Judge. Javier Luis, a resident of Florida, developed an online personal relationship with Ohio resident Catherine Zang. The relationship was apparently platonic, but Catherine's husband, Joseph Zang, was nonetheless suspicious of his wife's online activities. This caused Joseph to secretly install a product known as WebWatcher on the computer used by Catherine in order to monitor her communications. According to Luis, WebWatcher and its manufacturer, Awareness Technologies, Inc., surreptitiously intercepted the emails, instant messages, and other communications that were sent between Luis and Catherine. Awareness then allegedly disclosed the communications to Joseph, who used them as leverage to divorce Catherine on favorable terms.

Upset by the capture and disclosure of his otherwise private communications, Luis filed suit against Joseph Zang, Awareness, and several others. He eventually settled his claims against all the defendants other than Awareness. With respect to Awareness, Luis alleged that the involvement of its WebWatcher "spyware" in secretly recording the communications at issue violated the federal Wiretap Act, the Ohio Wiretap Act, and Ohio common law. The district court concluded that Luis had failed to state a cause of action against Awareness, leading to the present appeal. Because the district court's dismissal failed to take into account the extent to which Awareness itself was allegedly engaged in the asserted violations, we REVERSE the judgment of the district court and REMAND the case for further proceedings consistent with this opinion.

I. BACKGROUND

A. Factual background

This case is on appeal from the district court's order granting Awareness's motion to dismiss for failure to state a claim under Rule 12(b)(6) of the Federal Rules of Civil Procedure. The account that follows is consequently based on the facts as alleged in Luis's amended complaint. *See Boland v. Holder*, 682 F.3d 531, 534 (6th Cir. 2012) ("Like a district court

considering a motion to dismiss in the first instance, we accept all facts alleged in the complaint as true.").

In early 2009, Luis made contact with Catherine Zang while participating in an online "Metaphysics" chatroom hosted by America Online. Catherine at the time was married to Joseph Zang, but the marriage was not a happy one. This resulted in Luis reaching out to Catherine and "develop[ing] a caring relationship with her." The two never met in person, but they had "daily communications" that were sent via the internet between Luis's home in Florida and the Zang residence in Ohio.

Joseph suspected that Catherine was communicating with other men and decided to take steps to monitor Catherine's actions. He accordingly installed a software program known as "WebWatcher" on the computer used by Catherine. According to Luis's complaint, this program intercepts electronic communications such as emails and instant messages in real time as the communications are sent. The program then contemporaneously forwards the intercepted communications to servers maintained by Awareness in California, where the communications are stored for later review. A WebWatcher user such as Joseph may then access the servers and peruse copies of the communications at issue at any time after the communications are intercepted and stored.

Joseph allegedly installed WebWatcher on the computer used by Catherine sometime in early 2009, and he used the program to intercept emails and instant messages sent between Luis and Catherine for several months thereafter. He then used these communications as leverage to help his attorney secure favorable terms for a divorce from Catherine in 2010.

WebWatcher is manufactured and marketed by Awareness. The program allegedly "records all PC activity including emails, IMs, websites visited, web searches, Facebook/MySpace activity, and anything typed in real time." According to Awareness's advertisements, the WebWatcher program creates and stores a record of whatever is sent to or from the computer in question. The process occurs in "near real-time, even while [a] person is still using the computer." This means that even if a computer user deliberately deletes or fails to

save a communication, the WebWatcher program will record and save it for later retrieval from servers owned and maintained by Awareness.

The process also allows a WebWatcher user to access the communications from any location with an internet connection. Intercepted communications, in other words, are stored in and made available to the user from Awareness's servers, so a WebWatcher user can access the intercepted communications without physically accessing the computers that were used to send or receive those communications.

In addition, Awareness provides a service known as "Alert Word." This software program scans the captured communications and monitors them for certain keywords that may be of interest to the WebWatcher user. The program then takes screenshots of the relevant communications and highlights them so that the WebWatcher user can view the communications without sorting through material deemed irrelevant to the user.

According to Luis's complaint, Awareness markets the WebWatcher program as a means for suspicious spouses to illegally monitor their partners' communications without their partners' knowledge or consent. Luis specifically alleges that Awareness "intentionally targets their product at spouses in their marketing campaigns—enticing them with the lure of finding out *everything* that goes on in the targeted computer's private accounts." (Emphasis in original.) This marketing strategy allegedly goes "far beyond" any ostensibly legitimate purpose (such as monitoring a child's use of the Internet) that WebWatcher might otherwise have. Moreover, the marketing is allegedly similar to other companies' marketing strategies that the Federal Trade Commission has in the past condemned as encouraging illegal spying. Luis thus contends that Awareness "knew or should have known" that purchasers of WebWatcher "would use it for illegal purposes."

B. Procedural background

Luis became aware of Joseph's use of WebWatcher in the summer of 2010. He thereafter sued Awareness, Joseph, and several other defendants in the United States District Court for the Middle District of Florida. In August 2012, that court transferred the case to the United States District Court for the Southern District of Ohio.

As relevant to the current appeal, the complaint asserts three causes of action against Awareness. It first alleges that Awareness intentionally intercepted Luis's electronic communications, in violation of 18 U.S.C. § 2511 (part of the federal Wiretap Act). The complaint next alleges that Awareness violated 18 U.S.C. § 2512 (another part of the federal Wiretap Act) by manufacturing, marketing, selling, and operating a device that Awareness knew or had reason to know was to be used primarily for the surreptitious interception of electronic communications. Finally, the complaint asserts that Awareness violated Ohio state law by (1) intercepting and using his electronic communications within the meaning of Ohio's Wiretap Act, and (2) invading his privacy within the meaning of the common-law tort.

Awareness moved to dismiss Luis's complaint under Rule 12(b)(6) of the Federal Rules of Civil Procedure. It argued that (1) WebWatcher does not "intercept" communications as defined in the federal Wiretap Act, (2) Awareness cannot be held liable in a civil action because it did not "engage in" the alleged violation of the Act, and (3) Luis's factual allegations lacked enough detail to plead a claim under state law.

A magistrate judge was directed to prepare a Report and Recommendation (R&R) evaluating Awareness's arguments. The R&R concluded that Luis's communications had in fact been "intercepted" as that term is used in the federal Wiretap Act, but the magistrate judge nonetheless recommended that Luis's claims be dismissed. With respect to the claimed violation of 18 U.S.C. § 2511, the R&R concluded that Awareness itself did not "intercept" Luis's communications because it was Joseph—not Awareness—that installed the WebWatcher program on the computer used by Catherine. And with respect to the claimed violation of 18 U.S.C. § 2512, the R&R concluded that Awareness could not be held liable simply for manufacturing a product that others—such as Joseph—used to violate the Wiretap Act. The R&R further determined that Luis failed to allege sufficient facts to support any of his state-law theories of liability. As a result, the R&R concluded that all claims against Awareness should be dismissed.

The district court adopted the R&R in June 2014 and subsequently dismissed all claims against Awareness. Luis now appeals, arguing that he has adequately pleaded all three of the claims described above.

II. ANALYSIS

A. Standard of review

We review de novo the district court's decision to dismiss Luis's complaint under Rule 12(b)(6) of the Federal Rules of Civil Procedure. *See Kreipke v. Wayne State Univ.*, 807 F.3d 768, 774 (6th Cir. 2015). To survive a motion to dismiss under Rule 12(b)(6), a complaint must state a claim to relief that rises "above the speculative level" and is "plausible on its face." *Hensley Mfg. v. ProPride, Inc.,* 579 F.3d 603, 609 (6th Cir. 2009) (internal quotation marks omitted). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The complaint must therefore "contain either direct or inferential allegations respecting all material elements necessary for recovery under a viable legal theory." *Kreipke*, 807 F.3d at 774 (internal quotation marks omitted).

In evaluating a motion to dismiss, we "may consider the complaint and any exhibits attached thereto, public records, items appearing in the record of the case and exhibits attached to defendant's motion to dismiss so long as they are referred to in the complaint and are central to the claims contained therein." *Id.* (alterations and internal quotation marks omitted). We must accept the complaint's well-pleaded factual allegations as true, construe the complaint in the light most favorable to the plaintiff, and draw all reasonable inferences in the plaintiff's favor. *Bassett v. Nat'l Collegiate Athletic Ass'n*, 528 F.3d 426, 430 (6th Cir. 2008).

Moreover, Luis was acting pro se when he filed the relevant complaint in this case. We hold such pro se pleadings "to less stringent standards than formal pleadings drafted by lawyers." *Williams v. Curtin*, 631 F.3d 380, 383 (6th Cir. 2011) (internal quotation marks omitted). Luis's pleadings should therefore be "liberally construed." *See id.*

B. Luis sufficiently alleged facts supporting a cause of action against Awareness for illegal interception of an electronic communication, in violation of 18 U.S.C. § 2511

Luis's first claim is that Awareness violated 18 U.S.C. § 2511. That section reads as follows:

> (1) Except as otherwise specifically provided in this chapter[,] any person who—
> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . shall be punished [by a fine or by imprisonment.]

18 U.S.C. § 2511(1)(a). Section 2511 thus criminalizes the intentional interception of an electronic communication. *See id.* A separate section of the Wiretap Act then provides a private cause of action for persons who are victimized by such criminal conduct:

> (a) In general.—Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

18 U.S.C. § 2520(a).

Luis's first claim thus divides into two parts: one is the allegation that Awareness violated § 2511 by "intercepting" his communications, and the other is the allegation that, because Luis's communications were so intercepted, he has the right under § 2520 to pursue a private cause of action for that violation. Awareness does not challenge the second part of Luis's claim. In other words, Awareness concedes that if it is deemed to have intercepted Luis's communications in violation of § 2511, then Luis is entitled to bring a private cause of action against Awareness under § 2520 to redress that violation.

But Awareness does contest the first part of Luis's claim. It maintains that his claim falters because WebWatcher does not "intercept" electronic communications. Awareness asserts that the term "intercept" applies only to situations in which a device captures a communication "either before [the communication] reaches the intended recipient or contemporaneous with the transmission[,] but not after it reaches the destination where it is placed in electronic storage." It contends that WebWatcher does not satisfy this contemporaneity requirement because the device

ostensibly offers only the ability to "record[] various activities that occur" on a computer and then "review [those records] at a later date." Put differently, Awareness maintains that its device involves no "contemporaneous" capture of communications because "the user of Web Watcher cannot view [a] communication[] at the time the communication is transmitted." As explained below, Awareness correctly argues that the Wiretap Act imposes a contemporaneity requirement on the term "intercept," but Awareness is incorrect in arguing that Luis's allegations about WebWatcher fail to satisfy this requirement.

1. The term "intercept" as used in 18 U.S.C. § 2511 requires that an acquisition of a communication occur contemporaneously with the transmission of the communication

An "intercept" for purposes of the Wiretap Act is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). The Act does not explicitly require that the acquisition of a communication occur contemporaneously with the transmission of the communication. *See id.* Nonetheless, courts interpreting this language have uniformly concluded that an intercept requires contemporaneity. *See, e.g.*, *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003), *as amended* (Jan. 20, 2004) ("Every circuit court to have considered the matter has held that an 'intercept' under the [Act] must occur contemporaneously with transmission.").

The Fifth Circuit explained the basis for this requirement in *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994). In that case, the court observed that the Wiretap Act originally applied only to wire communications and oral communications. *Id.* at 461. Congress then passed the Electronic Communications Privacy Act (ECPA) in 1986, in which the Wiretap Act was amended to cover "electronic communications." *Id.*

In doing so, Congress drew a distinction between "electronic communications" and "electronic storage." *Id.* The former term is defined 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 photooptical system." 18 U.S.C. § 2510(12). In contrast, "electronic storage" is defined as "(A) any temporary, intermediate storage of a wire or

electronic communication incidental to the electronic transmission thereof," and "(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.* § 2510(17).

The term "intercept," as noted above, applies only to electronic communications, not to electronic storage. *See id.* § 2510(4). Applying this definition of intercept to the above-quoted definition of electronic communication thus means that the term intercept applies solely to the transfer of electronic signals. The term does not apply to the acquisition of electronic signals that are no longer being transferred.

This gives rise to the contemporaneity requirement. Once the transmission of the communication has ended, the communication ceases to be a communication at all. The former communication instead becomes part of "electronic storage." And at that point a person cannot "intercept" the former communication because the term intercept, as noted above, does not apply to electronic storage. Interception must thus occur contemporaneously with the transmission of the communication; it must, in other words, catch the communication "in flight" before the communication comes to rest and ceases to be a communication. *See Steve Jackson Games*, 36 F.3d at 461-62 ("Congress' use of the word 'transfer' in the definition of 'electronic communication', and its omission in that definition of the phrase 'any electronic storage of such communication'[,] . . . reflects that Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage'."); *see also United States v. Szymuszkiewicz*, 622 F.3d 701, 704 (7th Cir. 2010), *as amended* (Nov. 29, 2010) (concluding that "catching the message 'in flight'" constitutes an "unlawful interception").

This distinction between electronic communications and electronic storage is not an accident of statutory drafting. When Congress enacted the ECPA, it specifically differentiated between communications in transit and communications in storage. In particular, Title I of the ECPA prohibits intentionally intercepting electronic communications, whereas Title II of the ECPA prohibits gaining unauthorized access to stored communications. *See Steve Jackson Games*, 36 F.3d at 459. Title I, moreover, imposes certain procedural requirements on law-enforcement officers who wish to investigate crimes by intercepting electronic communications, whereas Title II implements different procedural requirements for law-enforcement officers who

wish to investigate crimes by accessing electronic storage. *Id.* at 463. Finally, Title I limits the types of crimes that can be investigated through the monitoring of electronic communications, but Title II contains no such limit on the types of crimes that can be investigated through access to stored communications. *Id.*

These distinctions between Title I and Title II of the ECPA show that Congress clearly meant to differentiate between communications and storage. The contemporaneity requirement thus plays a crucial role in effectuating congressional intent. If the communication is acquired contemporaneously with its transmission, then an "intercept" has occurred and Title I applies; in contrast, if the communication is not acquired contemporaneously with its transmission, then "storage" has been accessed and Title II applies. So even though the definition of "intercept" does not explicitly require that an acquisition be contemporaneous with transmission, *see* 18 U.S.C. § 2510(4), the contemporaneity requirement plays a key role in effectuating the design of the ECPA.

All of the circuit courts that have considered the issue have therefore followed *Steve Jackson Games* and have concluded, like the Fifth Circuit, that the acquisition of a communication must be contemporaneous with its transmission in order for an "intercept" to occur. *See Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003), *as amended* (Jan. 20, 2004) ("Nationwide argues that it did not 'intercept' Fraser's e-mail within the meaning of Title I because an 'intercept' can only occur contemporaneously with transmission . . . . [W]e agree with Nationwide."); *United States v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003) ("The Fifth and Ninth Circuits' reasoning is persuasive and we hold that a contemporaneous interception—*i.e.*, an acquisition during 'flight'—is required to implicate the Wiretap Act with respect to electronic communications."); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) ("We therefore hold that for a website . . . to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage."). *But see United States v. Councilman*, 418 F.3d 67, 79-80 (1st Cir. 2005) (casting doubt on the contemporaneity requirement, but ultimately concluding that the court "need not decide that question" on the facts of the case before it).

District courts in the Sixth Circuit have also adopted the contemporaneity requirement. *See, e.g.*, *Garback v. Lossing*, No. 09-CV-12407, 2010 WL 3733971, at *2 (E.D. Mich. Sept. 20, 2010) ("[Courts] agree that the term intercept encompasses only acquisitions contemporaneous with transmission. . . . [T]he Court finds this reasoning persuasive and adopts it here." (emphasis and internal quotation marks omitted)); *Cardinal Health 414, Inc. v. Adams*, 582 F. Supp. 2d 967, 979-80 (M.D. Tenn. 2008) ("The Third, Fifth, Ninth, and Eleventh Circuits all agree that, for a communication to be 'intercepted' under the [Wiretap Act], that communication must be acquired during the 'flight' of the communication. . . . The reasoning from the multiple circuit courts discussed above is sound . . . .").

Our court has not yet decided precisely when an "intercept" occurs under the Wiretap Act. In light of the above discussion, however, we conclude that the contemporaneity requirement is both (1) consistent with the structure of the ECPA, and (2) consistent with the interpretation of the Act adopted by every circuit to have ruled on the issue. We therefore hold that, in order for an "intercept" to occur for purposes of the Wiretap Act, the electronic communication at issue must be acquired contemporaneously with the transmission of that communication.

2. Luis's complaint sufficiently alleges that Awareness (via WebWatcher) acquires communications in a manner that is contemporaneous with their transmission

For the reasons explained above, Luis's claim that Awareness intercepted his electronic communications requires him to establish that Awareness acquired those communications contemporaneously with their transmission. Luis's complaint must therefore allege facts that, when accepted as true, give rise to a reasonable inference that Awareness contemporaneously acquired the communications. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Awareness argues that Luis's complaint fails to do so because (1) the complaint contains no specific allegations that WebWatcher contemporaneously captures communications, and (2) even if there are such allegations, those allegations are belied by an affidavit submitted by Awareness's Chief Executive Officer (CEO). Neither contention has merit.

a. Allegations of contemporaneous acquisition

In support of his illegal-intercept claim, Luis attached to his complaint various marketing materials that describe the features of a product called WebWatcher. As noted above, we may appropriately take account of such attachments. *See Kreipke v. Wayne State Univ.*, 807 F.3d 768, 774 (6th Cir. 2015) ("In reviewing a motion to dismiss, the Court may consider the complaint and any exhibits attached thereto . . . ." (alteration and internal quotation marks omitted)). Awareness, however, argues that the marketing materials in this case cannot be considered because they do not identify the source of the product. As stated by Awareness, the complaint contains "no allegation that they concern the product" that Joseph allegedly installed on the computer used by Catherine. It adds that "Luis uses [the] unverified marketing materials to form the basis of his Wiretap Act claims yet never makes the specific allegation that these marketing materials have any connection to the product used by Joseph C. Zang." Awareness therefore asks us to ignore these materials, maintaining that, in their absence, Luis's complaint lacks enough factual matter to state a valid claim.

We are not persuaded. Luis's complaint (1) specifically alleges that Awareness intercepted his communications using an electronic device called WebWatcher, (2) includes as attachments various marketing materials that describe the features of an electronic device unequivocally called WebWatcher, and (3) specifically refers to those marketing materials when describing the way in which Awareness's device operates. Thus, regardless of whether the complaint includes a specific allegation that the attached marketing materials refer to the same device identified in the body of the complaint, the only "reasonable inference" under these circumstances, *see Iqbal*, 556 U.S. at 678, is that they do.

Awareness is of course correct that some possibility exists that the marketing materials might refer to another device carrying the trademark "WebWatcher" that is unaffiliated with Awareness's own WebWatcher. This argument, however, is far-fetched at best, and the more "plausible inference," *see id.* at 682, is that the materials do in fact apply to Awareness's WebWatcher that Joseph allegedly used. These materials thus help illuminate the way in which WebWatcher allegedly intercepted Luis's communications.

In addition, Luis at this point in the litigation need push his claim past only the "speculative level." *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) ("Factual allegations must be enough to raise a right to relief above the speculative level . . . ."). Hence, even if there exists some minimal doubt about the relationship between Awareness's WebWatcher and the WebWatcher marketing materials attached to the complaint, that doubt, standing alone, is not enough to ignore the materials. This is especially true because we must liberally construe Luis's pro se complaint, *see Williams v. Curtin*, 631 F.3d 380, 383 (6th Cir. 2011), with the result that we will grant Luis the benefit of any doubt and conclude that, for the purposes of the current appeal, the marketing materials do in fact apply to the WebWatcher at issue.

We next consider whether the marketing materials and Luis's accompanying allegations contain factual content sufficient to support a reasonable inference that Awareness, via WebWatcher, acquired Luis's electronic communications contemporaneously with their transmission. Two allegations in the complaint support this inference. First, Luis alleges that the communications at issue "were not originally stored on the computer's hard drive." The communications were instead acquired by Awareness "as [they were] being written and communicated between senders and recipients." This allegation directly supports the proposition that the communications were still "in flight" for the purposes of 18 U.S.C. § 2511. *See United States v. Szymuszkiewicz*, 622 F.3d 701, 704 (7th Cir. 2010), *as amended* (Nov. 29, 2010) (noting that "catching the message 'in flight'" constitutes an "unlawful interception" under § 2511); *United States v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003) ("[W]e hold that a contemporaneous interception—*i.e.*, an acquisition during 'flight'—is required to implicate the Wiretap Act with respect to electronic communications.").

Second, Luis alleges that "WebWatcher immediately and *instantaneously* rout[e]s the intercepted communications to their [i.e., Awareness's] servers located in California." (Emphasis in original.) This allegation directly supports an inference of contemporaneous interception because, if WebWatcher does in fact "immediately and *instantaneously*" copy and send communications "as [they are] being written," then the acquisition of the communications likely occurs before the communications have come to rest in electronic storage. In turn, this

allegation supports a reasonable inference that the communications have in fact been intercepted for the purposes of § 2511. *See Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 461-62 (5th Cir. 1994) (drawing a distinction between (1) acquiring an electronic communication, which is an intercept, and (2) accessing electronic storage, which is not).

The marketing materials attached to Luis's complaint support this conclusion. As Luis notes, the materials state that WebWatcher lets its users review a person's electronic communications "in near real-time, even while the person is still using the computer." The materials further note that any deviation from real-time monitoring results not from delays regarding when the communications are acquired, but from variations in "the Internet connection speed of the computer being monitored."

This near real-time monitoring is significant. If a WebWatcher user can in fact review another person's communications in near real time, then WebWatcher must be acquiring the communications and transferring them to Awareness's servers as soon as the communications are sent. The program, in other words, does not wait for the communications to be stored; instead, the program as described captures and reroutes the communications so that a WebWatcher user can review the communications at nearly the same time as they are being transmitted.

In addition, the marketing materials state that "[e]ven if a document is never even saved, WebWatcher still records it." This feature indicates that WebWatcher does not wait for electronic communications to be saved in a computer's electronic storage. Rather, the product records the communications as they are being sent, without regard for whether a copy is ever placed in the storage of the affected computer. This aspect of WebWacher's operations thus implies that the alleged acquisition of Luis's communications indeed occurred while the communications were still "in flight." *See Szymuszkiewicz*, 622 F.3d at 704. And this allegation, in connection with the other allegations described above, supports a reasonable inference that Luis's communications were in fact "intercepted" under 18 U.S.C. § 2511.

Nor do other allegations in the complaint undermine this conclusion. At oral argument, an issue was raised about the effect of the complaint's later reference to "oral" communications.

Paragraph 98 of the complaint, for instance, states that "Defendants, and each of them," violated the Wiretap Act because they "intentionally intercepted . . . oral communication[s]," or "intentionally disclosed . . . oral communication[s]," or "intentionally used . . . the contents of oral communication[s]." These allegations regarding oral communications, the argument goes, are inconsistent with Luis's basic claim that his electronic communications—such as emails and instant messages—were intercepted by Awareness, with the result that Luis's claims purportedly do not state a plausible basis for relief.

We respectfully disagree. Although Paragraph 98 does refer to oral communications, that paragraph also "restates and re-alleges the allegations set forth" in the complaint's preceding paragraphs. And in those paragraphs, Luis specifically alleges that the "listed defendants . . . violated the federal wiretap law . . . when *electronic communications* originating from Plaintiff's computer located in Florida[] were intercepted in transmission using WebWatcher." (Emphasis added.) Luis then adds that the electronic communications sent between Luis and Catherine were intercepted when WebWatcher sent those communications to Awareness's servers in California. The complaint thus in fact alleges that Luis's electronic communications were intercepted by Awareness, with the result that the references to oral communications later in the complaint do not defeat the conclusion that Luis has stated an adequate claim under 18 U.S.C. § 2511.

b. The affidavit from Awareness's CEO

Awareness resists the above conclusion that an intercept occurred by relying on an affidavit submitted by its CEO, Brad Miller. This affidavit was executed in August 2012 and is attached to Awareness's motion to dismiss. Miller states in the affidavit that, after being installed on a computer, WebWatcher "records various activities . . . such as e-mails sent and received, websites visited, keystrokes typed and transcripts of online chats." This recorded content is then "sent to an online account," from which a WebWatcher user may access the material at a later date. According to Miller, a WebWatcher user "cannot view communications at the time a communication is transmitted."

This purported lack of real-time monitoring is important, Awareness maintains, because it allegedly shows that any acquisition of communications is not contemporaneous with the communications' transmission. Awareness thus urges that Miller's affidavit be read as firmly establishing that no contemporaneous acquisition—and hence no intercept—occurred in this case.

This argument is unpersuasive for two reasons, the first procedural and the second substantive. Procedurally, Awareness is not entitled to rely on affidavits at this stage of the case. A court evaluating a motion to dismiss may, as noted above, consider "the complaint and any exhibits attached thereto, public records, items appearing in the record of the case and exhibits attached to defendant's motion to dismiss so long as they are referred to in the complaint and are central to the claims contained therein." *Kreipke v. Wayne State Univ.*, 807 F.3d 768, 774 (6th Cir. 2015) (alterations and internal quotation marks omitted). Miller's affidavit, although attached to Awareness's motion to dismiss, is plainly not "referred to in the complaint." The affidavit therefore does not fall within the categories of documents that may be considered at this point in the litigation. *See id.*

Rule 12(d) of the Federal Rules of Civil Procedure confirms this conclusion. That rule provides that if, "on a motion under Rule 12(b)(6) or 12(c), matters outside the pleadings are presented to and not excluded by the court, the motion must be treated as one for summary judgment under Rule 56." The Miller affidavit is a "matter[] outside the pleadings," so the district court had the option of either excluding the affidavit or converting Awareness's motion to one for summary judgment. *See Dayco Corp. v. Goodyear Tire & Rubber Co.*, 523 F.2d 389, 392 (6th Cir. 1975) ("It seems clear then, that if affidavits are filed with the district court, the court must proceed under Rule 56 unless the court decides to exclude the affidavits."). Nothing in the record suggests that the district court proceeded under Rule 56, so the Miller affidavit is not a proper basis on which to resolve Awareness's motion to dismiss. *See id.*; *see also Tackett v. M & G Polymers, USA, LLC*, 561 F.3d 478, 488 (6th Cir. 2009) ("Because the district court's ruling was not the functional equivalent of a Rule 56 ruling, we decline the Defendants' invitation to base our ruling on Rule 56. Therefore, we will not consider matters extrinsic to the pleadings . . . .").

Moreover, even if we were to consider Miller's affidavit, the substance of Awareness's argument is lacking. The affidavit states that WebWatcher "records various activities" on a computer and then sends those records to servers maintained by Awareness. But the affidavit does not specify how or when WebWatcher actually creates the records of the affected computer's activities. The affidavit therefore does not foreclose the possibility that WebWatcher acquires electronic communications before they come to rest in electronic storage. In other words, the acquisition might still be contemporaneous with the communications' transmissions.

And even if Miller is correct that a WebWatcher user "cannot view communications at the time a communication is transmitted," that assertion does not necessarily undermine Luis's allegations. Luis claims that Awareness itself illegally intercepted his communications, and he specifically alleges that Awareness—through WebWatcher—"immediately and *instantaneously* rout[e]s the intercepted communications to their servers located in California." (Emphasis in original.) Hence, even if a WebWatcher *user* cannot obtain real-time access to the communications, the possibility remains that Awareness *itself* acquires the communications while they are still in transit. Any potential delay in access to the communications for a WebWatcher user therefore does not preclude a finding that Awareness itself acquires the communications in a manner contemporaneous with their transmission.

For the above reasons, neither Awareness's arguments about the complaint's allegations nor its reliance on its CEO's affidavit is persuasive. We therefore reject Awareness's assertions with respect to Luis's claim under § 2511.

3. The district court's erroneous conclusion

In ruling on Awareness's motion to dismiss, the district court largely agreed with the above analysis and concluded that Luis's communications had been intercepted. The court nonetheless granted Awareness's motion to dismiss Luis's § 2511 claim on the ground that "[Awareness] itself cannot be deemed to have 'intercepted' any of Plaintiff's communications." Instead, the court attributed liability for the intercept solely to Joseph, the WebWatcher user.

Where the district court erred was in failing to recognize that Luis alleges not only that Awareness manufactures and sells WebWatcher, but that, once installed on a computer,

WebWatcher automatically acquires and transmits communications to servers that Awareness owns and maintains. The alleged intercept of a communication thus occurs at the point where WebWatcher—without any active input from the user—captures the communication and reroutes it to Awareness's own servers. Construing these allegations liberally, as we must under *Williams v. Curtin*, 631 F.3d 380, 383 (6th Cir. 2011), the complaint supports an inference that Awareness itself—not simply the WebWatcher user—"acquires" the communications by rerouting them to servers that it owns and controls. That, in turn, suggests that Awareness itself is responsible for the alleged intercept. *See* 18 U.S.C. § 2510 (defining "intercept" as the "acquisition" of a communication). Put differently, the complaint's focus on Awareness's continued operation of the WebWatcher program—even after that program is sold to a user—convinces us that Luis has plausibly pleaded that Awareness intercepted his communications.

And that gives rise to a plausible claim for relief. This is because Awareness, as noted above, does not contest the proposition that if Awareness itself is deemed to have violated § 2511 by intercepting Luis's communications, then Luis may sue Awareness under § 2520 to redress that violation. For the reasons explained above, we conclude that Luis has indeed alleged enough facts to reasonably infer that Awareness intercepted his communications. Luis may therefore proceed with his private cause of action on the basis of Awareness's alleged violation of § 2511.

The dissent disputes our conclusion on the ground that Luis "simply does not allege that Awareness was the one intentionally doing the intercepting." Dissenting Op. 33. Its grammatical basis for this critique stems from the statement in the complaint that "WebWatcher . . . routs the intercepted communications to their servers" to be stored and analyzed for "their subscribers." *Id.* at 2. The dissent concludes that there is no plausible connection between Awareness and the subject of the pronoun "their." *See id.*

To the contrary, paragraphs 12 and 96 of the complaint specifically allege that Awareness (1) manufactures WebWatcher, (2) conducts "all marketing" for WebWatcher, and (3) is the "parent company" of WebWatcher. Hence, when Luis alleges that "WebWatcher . . . routs the intercepted communications" to "their" servers for "their" subscribers, the most plausible inference is that the word "their" applies to both WebWatcher and Awareness. Such a "plausible

inference" is all that is required to survive a motion to dismiss, *see Iqbal*, 556 U.S. at 682, so the dissent's argument does not persuade us that Luis's complaint is deficient.

C. Luis sufficiently alleged facts supporting a cause of action against Awareness for manufacturing, marketing, selling, and operating a wiretapping device in violation of 18 U.S.C. § 2512(1)(b)

The second claim that Luis pursues on appeal is that Awareness violated 18 U.S.C. § 2512(1)(b), and that this violation gives rise to a private cause of action for a party in Luis's circumstances. Section 2512(1)(b) reads as follows:

> Except as otherwise specifically provided in this chapter, any person who intentionally . . . (b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications . . . shall be fined under this title or imprisoned not more than five years, or both.

Luis's complaint plainly alleges facts that support a reasonable inference that Awareness violated this section. First, Luis claims that Awareness is the manufacturer of WebWatcher, a device specifically designed to surreptitiously "intercept[] communications" such as those that were electronically transmitted between Luis and Catherine. Second, Luis claims that Awareness markets WebWatcher as a means for one spouse to illegally monitor the communications of another spouse in a way that goes "far beyond" any legitimate purpose that WebWatcher might have. These allegations easily support an inference that Awareness manufactures a device "knowing or having reason to know" that the device is "primarily useful for . . . the surreptitious interception of . . . electronic communications." The complaint therefore adequately alleges a violation of 18 U.S.C. § 2512(1)(b).

This leads to the question whether Luis can sue for that violation. Section 2512(1)(b) itself does not allow for such a suit because it provides only that the violator will be "fined . . . or imprisoned." Luis's private cause of action for such a violation thus depends on the proper interpretation of 18 U.S.C. § 2520.

Section 2520, as noted previously, states that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of [the Wiretap Act]

may in a civil action recover from the person or entity . . . which engaged in that violation such relief as may be appropriate." For the reasons explained earlier, Luis has adequately alleged facts supporting an inference that he is a "person whose . . . electronic communication [was] intercepted . . . in violation" of the Wiretap Act. *See* Part II.B. above. Luis is accordingly entitled to recover from the "person or entity . . . which engaged in that violation." The sole question in assessing Luis's § 2512(1)(b) claim is therefore whether Awareness's alleged manufacture, marketing, sale, and operation of WebWatcher caused it to be "engaged in that violation" of the Wiretap Act when Luis's communications were intercepted.

Awareness argues that manufacturing an electronic device does not amount to such engagement within the meaning of § 2520. It observes that § 2520 provides recovery for a plaintiff whose communication is "intercepted, disclosed, or intentionally used," which it contends should limit liability to those defendants who actually initiate the interception, disclosure, or intentional use at issue. Because manufacturing an electronic device is different than "intercepting, disclosing, or intentionally using" a communication, Awareness argues that § 2520 provides no private cause of action against a manufacturer that violates § 2512(1)(b).

Luis counters that Awareness's interpretation ignores the plain language of the statute. If Congress had meant to restrict liability to only those persons or entities who make the specific decision to "intercept, disclose, or intentionally use" a communication, then Congress would have used those terms in defining the class of defendants subject to suit under § 2520. But as Luis notes, Congress eschewed that route. Congress instead chose to impose liability on any person or entity that "engaged in" the interception, disclosure, or intentional use of the communication in question. Stated differently, Luis contends that Congress's definition of the class of defendants as those who "engage[] in" certain Wiretap Act violations is broad enough to include those entities—such as Awareness—that allegedly violate § 2512(1)(b) by manufacturing and remaining involved in the operation of a device that is primarily used to commit such violations.

Courts that have previously addressed these arguments have come to inconsistent conclusions. On the one hand, a number of district courts have adopted a broad reading of § 2520 by concluding that the section gives rise to a private cause of action against anyone who

violates the Wiretap Act, regardless of whether that violation was specifically an intercept, disclosure, or use of a communication. *See, e.g.*, *DIRECTV, Inc. v. Dougherty*, No. 1:02-CV-05576, 2003 WL 24046760, at *2-3 (D.N.J. Oct. 8, 2003) (concluding that "[a]nyone who violates a provision of the ECPA is a potential defendant," and describing this conclusion as "the majority position" and "the better view"); *see also DIRECTV, Inc. v. Kitzmiller*, No. CIV.A. 03-3296, 2004 WL 692230, at *4 (E.D. Pa. Mar. 31, 2004) (agreeing with *Dougherty* that "anyone who violates a provision of the ECPA is a potential defendant" and stating that "this newly-developed majority view is the better approach"). These courts, for example, have imposed civil liability for simply possessing a wiretapping device in violation of § 2512(1)(b), even though such possession, standing alone, does not involve the intercept, disclosure, or use of a communication. *See Dougherty*, 2003 WL 24046760, at *2 ("[T]he recently developed majority view is that § 2520(a) does allow for the recovery of damages against one who possesses an intercepting device.").

On the other hand, two of our sister circuits have disagreed with the conclusion reached by cases such as *Dougherty* and *Kitzmiller*. These circuits hold that § 2520 provides a cause of action against only those defendants whose violation of the Wiretap Act consists of an intercept, disclosure, or intentional use of a communication. Other violations, such as the simple possession of a wiretapping device, do not give rise to civil liability. *See DirecTV, Inc. v. Treworgy*, 373 F.3d 1124, 1127 (11th Cir. 2004) ("The phrase 'which engaged *in that violation*' makes apparent the intent of Congress to limit liability to a certain class of defendants. Congress chose to confine private civil actions to defendants who had 'intercepted, disclosed, or intentionally used a communication in violation of . . . [the Wiretap Act.]'" (emphasis in original) (citations and some alterations omitted)); *see also DIRECTV Inc. v. Robson*, 420 F.3d 532, 539 & n.31 (5th Cir. 2005) (collecting cases that have found "no merit in [the] assertion that § 2520 expressly provides a private cause of action for [all] violations of the criminal proscriptions of § 2512" (alterations, citation, and internal quotation marks omitted)).

These conflicting arguments have generated divergent results in the context of private suits alleging that a defendant violated § 2512(1)(b) simply by possessing a device that is primarily used for surreptitious wiretapping. Those courts that accept a broad reading of the

"engaged in" language hold that possession of such a device, without more, is indeed enough to support a private cause of action under § 2520. *See Dougherty*, 2003 WL 24046760, at *2 (collecting cases in which courts have found "that § 2520(a) does subject possessors of intercepting devices to civil liability").

In contrast, those courts that adopt a more limited reading of the "engaged in" language hold that simple possession is not enough to support a private cause of action for a violation of § 2512(1)(b). *See, e.g.*, *Treworgy*, 373 F.3d at 1129 ("Because the language of section 2520(a) does not create a private right of action against a person who possesses a device in violation of section 2512(1)(b), we cannot create one."); *Directv, Inc. v. Amato*, 269 F. Supp. 2d 688, 691 (E.D. Va. 2003) ("[T]he mere *possession* of such a device, as banned by § 2512, creates . . . no justification for private recovery." (emphasis in original)). Possession of a wiretapping device, in other words, can constitute a violation of the Wiretap Act, *see* 18 U.S.C. § 2512(1)(b), but this violation does not give rise to a private cause of action because "possession" of such a device is distinct from "intercepting, disclosing, or intentionally using" a communication.

We conclude that the Eleventh Circuit and those other courts that have adopted a narrow reading of § 2520 have the better end of this debate. This is because the phrase "engaged in that violation" plainly refers back to the earlier clause defining the "violation" as an "intercept[], disclos[ure], or intentional[] use[]." *See* 18 U.S.C. § 2520. The earlier clause thus defines the scope of the phrase "engaged in that violation," with the implication that a court should not read the latter phrase as imposing liability for violations such as simple possession of a wiretapping device. *See Treworgy*, 373 F.3d at 1127 ("As explained by one district court, as a matter of grammar and sentence structure, the phrase 'that violation' refers to the interception, disclosure, or intentional use of communications mentioned earlier in the sentence, and not to the possession of prohibited devices." (citation, emphasis, and internal quotation marks omitted)).

Our narrow reading of § 2520, however, does not doom Luis's claim. This is because the facts of the current case are materially different from the facts of cases such as *Treworgy*. In the latter cases, the courts were focused on whether a defendant's possession of a wiretapping device, without more, was sufficient to support a private cause of action. *See id.* at 1125 ("The issue presented by this interlocutory appeal [is] . . . whether 18 U.S.C. section 2520(a), as

amended in 1986, provides a private right of action against persons who possess devices used to intercept satellite transmissions in violation of 18 U.S.C. section 2512(1)(b), a criminal offense."); *see also DIRECTV Inc. v. Robson*, 420 F.3d 532, 539 & n.31 (5th Cir. 2005) (citing *Treworgy* for the proposition that "the civil cause of action embodied in § 2520 does not cover . . . possessory violations").

The present case, in contrast, involves much more than simple possession. Instead, as described above, Awareness allegedly manufactured, marketed, and sold WebWatcher with knowledge that it would be primarily used to illegally intercept electronic communications. It then remained actively involved in the operation of WebWatcher by maintaining the servers on which the intercepted communications were later stored for WebWatcher's users. Awareness thus allegedly took a much more active role in causing the Wiretap Act violation in this case than the defendants in other cases who did nothing more than possess a wiretapping device in contravention of § 2512(1)(b).

We accordingly emphasize that our narrow holding is consistent with the conclusion that § 2520 does not support a cause of action against those who simply possess a wiretapping device. Instead, we today hold that a defendant such as Awareness—which allegedly violates § 2512(1)(b) by manufacturing, marketing, and selling a violative device—is subject to a private suit under § 2520 only when that defendant also plays an active role in the use of the relevant device to intercept, disclose, or intentionally use a plaintiff's electronic communications.

So even though Awareness itself did not initiate the specific action that "intercepted, disclosed, or intentionally used" Luis's communications in violation of the Wiretap Act, it is alleged to have actively manufactured, marketed, sold, and operated the device that *was used* to do so. This is enough to establish that Awareness was "engaged in" a violation of the Wiretap Act in a way that defendants such as those in *Treworgy* and *Amato*—who simply possessed wiretapping devices—were not. *See DirecTV, Inc. v. Tasche*, 316 F. Supp. 2d 783, 790 (E.D. Wis. 2004) ("Though Tasche may not have actually done the intercepting himself, it would be a stretch to find that he was not 'engaged in' that act. Those who sell devices that are designed to steal DirecTV's satellite transmissions to those who are intent on stealing DirecTV's satellite transmissions are, in my view, 'engaged in' intercepting such transmissions.").

The dissent disputes the outcome that we reach on this issue, contending that civil liability under §§ 2512(1)(b) and 2520 should extend only to those persons or entities who themselves intercept, disclose, or use a would-be plaintiff's electronic communication. Dissenting Op. 35. As support, the dissent relies on *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158 (5th Cir. 2000), and *Flowers v. Tandy Corp.*, 773 F.2d 585 (4th Cir. 1985), which purportedly are consistent with the dissent's narrow conception of §§ 2512(1)(b) and 2520. We find both cases readily distinguishable.

In *Peavy*, the plaintiffs sought to pursue a civil action for an alleged violation of § 2511(1)(a). 221 F.3d at 167. That section provides in pertinent part that a Wiretap Act violation occurs if a person "procures any other person to intercept . . . any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). The plaintiffs thus argued that the defendants were liable in a civil action brought under § 2520 because the defendants had "procured" others to intercept the plaintiffs' communications. 221 F.3d at 167-68.

On appeal, the Fifth Circuit considered whether § 2520 was broad enough to encompass defendants accused of violating § 2511(1)(a) via procurement. *Id.* The court observed that, prior to 1986, § 2520 read as follows:

> Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) 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 communications, and (2) be entitled to recover from any such person [damages, attorney's fees, and costs].

18 U.S.C. § 2520 (1970) (emphasis added). In 1986, however, Congress amended § 2520. Hence, both at the time that *Peavy* was decided and as currently written, § 2520 reads in relevant part as follows:

> [A]ny person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity . . . which engaged in that violation such relief as may be appropriate.

18 U.S.C. § 2520 (2012).

The Fifth Circuit found the difference between the two versions of the statute significant. It noted that the 1986 amendment specifically deleted the reference to "procuring" the intercept of an electronic communication, with the implication that Congress—by making that deletion—intended to foreclose civil liability for such conduct. 221 F.3d at 169 (reading the 1986 amendment as a sign that Congress meant "to take away a civil action for procurement").

The civil action in the current case rests on a different statutory footing. Luis argues—and we conclude—that his complaint adequately alleges that Awareness "engaged in" a violation of the Wiretap Act. As opposed to the "procurement" language at issue in *Peavy*, the "engaged in" language was not deleted from the earlier version of § 2520; instead, the "engaged in" language was specifically *added* when Congress enacted the 1986 amendment. The current case is thus easily distinguishable from *Peavy* because there exists no implication that Congress intended to foreclose claims such as Luis's by altering the language of § 2520.

Flowers is likewise distinguishable. In that case, as in *Peavy*, the court considered the pre-1986 version of § 2520. *See* 773 F.2d at 587 & n.2. That version of the statute, as noted above, explicitly limited the defendants that could be held liable in a civil action to those persons or entities who themselves "intercept[ed], disclose[d], or use[d]" electronic communications, "or procure[ed] any other person to intercept, disclose, or use such communications." 18 U.S.C. § 2520 (1970). The current version of the statute, however, contains no such explicit delineation of the activities that give rise to civil liability. *See* 18 U.S.C. § 2520 (2012). As a result, Luis's claim in this case rests on a much firmer statutory foundation than the claim that was at issue in *Flowers*.

Moreover, the relevant claim in *Flowers* was an assertion that the defendant had sold a device that was later used by the purchaser to violate the Wiretap Act. 773 F.2d at 589. The Fourth Circuit ultimately concluded that this claim failed because the sale of the device, without additional conduct by the seller and without its knowledge of the device's intended use, did not give rise to liability. *Id.* at 590 (finding no liability for "the mere selling" of the device); *see also id.* at 591 (concluding that the seller could not be held liable when it lacked "any knowledge of [the] intended use of the device").

Luis's claim, in contrast, is not limited to "the mere selling" of the device at issue. Rather, Luis claims that Awareness manufactured, marketed, sold, and *actively operated* the violative device, all while *knowing* that its device was to be used primarily for the surreptitious interception of electronic communications. Awareness's alleged conduct in this case, in other words, is far more culpable than the defendant's alleged conduct in *Flowers*, with the result that *Flowers* sheds little light on whether Luis has stated a claim under §§ 2512(1)(b) and 2520.

The dissent next asserts that our analysis "confuses Awareness's alleged violations of § 2512 with violations of § 2511." Dissenting Op. 36. We respectfully disagree because Luis's claims, as explained below, are analytically distinct.

First, Luis alleges that Awareness violated § 2511 when Awareness itself intercepted his electronic communications in violation of the Wiretap Act. *See* Part II.B. above. But regardless of the outcome of the § 2511 claim, Luis has also alleged a violation of § 2512. He asserts that, by manufacturing, marketing, selling, and actively operating the wiretapping device at issue, Awareness (1) violated § 2512, and (2) "engaged in" the illegal intercept of Luis's communications. Hence, even if a jury ultimately concludes that only Zang (and not Awareness) intercepted Luis's communications in violation of § 2511, Awareness might still be liable because it "engaged in" that violation (*see* § 2520) by manufacturing, marketing, selling, and actively operating the device that was used by Zang to conduct the intercept. Luis's two claims, in other words, do not rise and fall together.

Finally, the dissent asserts that our reading of the statute interjects unwarranted "indeterminacy" into the evaluation of private suits for claimed violations of § 2512. Dissenting Op. 37. We again respectfully disagree. The essence of our holding is that a defendant who manufactures, markets, and sells a wiretapping device in violation of 18 U.S.C. § 2512 is potentially liable in a private suit brought under § 2520 when that defendant also plays an active role in the operation of the device to "intercept, disclose, or intentionally use" a plaintiff's electronic communications. Put differently, the active operation of the device establishes that a defendant who has manufactured, marketed, and sold the device at issue (in violation of § 2512) has in fact participated in the intercept, disclosure, or use of a plaintiff's communications to such a degree that the defendant has "engaged in" the underlying violation. Manufacturing,

marketing, and selling the device is thus a necessary prerequisite for a civil suit for a violation of § 2512; and, when that prerequisite is combined with the defendant's active operation of the device at issue, the defendant's conduct suffices to satisfy the "engaged in" standard of § 2520.

As the dissent observes, Dissenting Op. 36, this standard may in some cases raise factual questions about whether a defendant's role in operating a wiretapping device is extensive enough to constitute "engaging in" the underlying violation of the Wiretap Act. But such disputes are no different than any case in which a court or jury is called on to decide whether certain conduct falls within a statutory definition. We accordingly doubt that the district courts will have any difficulty when applying this standard. For all of these reasons, we reverse the judgment of the district court with respect to the dismissal of Luis's § 2512 claim.

D. Luis sufficiently alleged facts supporting his causes of action under the Ohio Wiretap Act and Ohio common law

In addition to his federal claims under the Wiretap Act, Luis's complaint contains a number of claims brought under Ohio state law. The district court dismissed all of his state-law claims. On appeal, Luis raises only two of them: (1) the alleged violations of the Ohio Wiretap Act, and (2) the tortious invasion of his privacy.

1. Luis sufficiently pleaded a cause of action under Ohio Rev. Code Ann. § 2933.52

Luis argues that his complaint states a claim under two different subsection of the Ohio Wiretap Act: § 2933.52(A)(1) and § 2933.52(A)(3). Subsection (A)(1) provides that "[n]o person purposely shall . . . intercept a wire, oral, or electronic communication," and subsection (A)(3) states that no person shall "[u]se . . . the contents of a wire, oral, or electronic communication, knowing or having reason to know that the contents were obtained . . . in violation of [the Ohio Wiretap Act.]"

a. Purposeful intercept under § 2933.52(A)(1)

As Luis notes, § 2933.52(A)(1) of the Ohio Wiretap Act closely parallels the language of 18 U.S.C. § 2511. *Compare* 18 U.S.C. § 2511(1)(a) (imposing a penalty on persons who "intentionally intercept[] . . . any wire, oral, or electronic communication"), *with* Ohio Rev. Code

Ann. § 2933.52(A)(1) (providing that no person shall "purposely . . . intercept a wire, oral, or electronic communication"). The Acts also use nearly identical definitions of the terms "intercept" and "device." *Compare* 18 U.S.C. § 2510(4)-(5) *with* Ohio Rev. Code Ann. § 2933.51(C)-(D). Thus, for the same reasons that Luis's allegations state a claim for relief under 18 U.S.C. § 2511, *see* Part II.B. above, Luis's allegations state a claim for relief under § 2933.52(A)(1) of the Ohio Wiretap Act. *Cf. Nix v. O'Malley*, 160 F.3d 343, 348 (6th Cir. 1998) (construing § 2933.52(A)(2) and (A)(3) of the Ohio Wiretap Act as "mirroring" or as being "equivalent to" the federal Wiretap Act).

Consistent with its rulings on Luis's federal claims, the district court held that the Ohio Wiretap Act "does not contemplate imposing civil liability on software manufacturers and distributers for the activities of third parties." The court thus concluded that Awareness could not be held liable for Joseph's actions in installing and using WebWatcher.

This reasoning is erroneous because Luis does not allege that Awareness is liable solely on the basis of Joseph's actions. Luis instead alleges that Awareness itself violated the Act in question. In particular, Luis's instant messages, emails, and other electronic communications were allegedly forwarded to Awareness's own servers in California. The messages were then allegedly (1) stored for later disclosure to Joseph, and (2) subjected to Awareness's "Alert Word" filtering system. Based on these allegations, Awareness itself "acquir[ed] . . . the contents of . . . [Luis's] electronic communications" and thus "intercepted" the communications within the meaning of the Ohio Wiretap Act. *See* Ohio Rev. Code Ann. § 2933.51(C) (defining "intercept" as "the aural or other acquisition of the contents of any wire, oral, or electronic communication"). Luis's complaint could admittedly be clearer on this point, but we must construe Luis's pro se pleading liberally. *See Williams v. Curtin*, 631 F.3d 380, 383 (6th Cir. 2011). We thus conclude that the district court erred and that Luis has adequately stated a claim for relief on the ground that Awareness itself allegedly intercepted Luis's communications in violation of § 2933.52(A)(1).

b. Unauthorized use of the contents of an electronic communication under § 2933.52(A)(3)

Luis's second theory of liability under the Ohio Wiretap Act is that Awareness illegally "used" the contents of his electronic communications. This theory has three requirements. Luis must first allege that Awareness "used" an intercepted communication as that term has been defined for the purposes of § 2933.52(A)(3). He must next allege that the interception that captured the communication was itself a violation of the Ohio Wiretap Act. *See Nix*, 160 F.3d at 348. Finally, Luis must allege that Awareness knew or had reason to know of the violation at the time that it used the intercepted communication. *See id.*

Luis alleges that Awareness "used" his communications when Awareness stored them on its servers in California and then disclosed them to Joseph for his later review. Ohio has treated the disclosure of an intercepted communication as conduct that satisfies the "use" requirement for the purposes of the Ohio Wiretap Act. *See Nix*, 160 F.3d at 348 ("In 1996, Ohio replaced section 2933.52(A)(3)'s prohibition on 'disclosure' with a prohibition on 'use,' but . . . the district court and all parties have consistently interpreted § 2933.52(A)(3) to prohibit both use and disclosure . . . ."). In addition, Awareness does not challenge this interpretation of "use." Luis has thus satisfied the first requirement for pleading a cause of action under § 2933.52(A)(3).

Next, Luis sufficiently alleged that Awareness itself violated the Ohio Wiretap Act by intercepting his communications within the meaning of § 2933.52(A)(1). *See* Part II.D.1.a. above. Moreover, even if Luis's theory of direct liability for Awareness ultimately proves untenable, he has alleged that Joseph also violated § 2933.52(A)(1) by intercepting Luis's electronic communications. Luis has therefore satisfied the second requirement of § 2933.52(A)(3) by alleging that his electronic communications were indeed intercepted in violation of the Ohio Wiretap Act.

Finally, Luis's complaint alleges that Awareness markets WebWatcher with the expectation that purchasers will use the program for surreptitiously monitoring the communications of other persons. He claims in particular that Awareness "intentionally targets [its] product at spouses in [its] marketing campaigns—enticing them with the lure of finding out *everything* that goes on in the targeted computer's private accounts." (Emphasis in original.)

This marketing, Luis alleges, goes "far beyond" any legal uses that the product might have and is reminiscent of advertising strategies that the Federal Trade Commission has previously condemned as encouraging illegal spying.

Assuming that these allegations accurately describe Awareness's marketing efforts—as we must at this point in the litigation, *see Boland v. Holder*, 682 F.3d 531, 534 (6th Cir. 2012) ("[W]e accept all facts alleged in the complaint as true.")—Awareness would have had a "reason to know" that any communications that it obtained through WebWatcher were obtained in violation of the Ohio Wiretap Act. Luis has therefore adequately pleaded the third requirement to establish liability under § 2933.52(A)(3). We accordingly reverse the district court's dismissal of this claim.

2. Luis sufficiently pleaded invasion of privacy under Ohio common law

Luis's final argument is that he has sufficiently pleaded a claim for common-law invasion of privacy. The parties agree that Ohio recognizes the "intrusion" variant of this tort. Prevailing on an intrusion claim requires the plaintiff to show that the defendant caused a "wrongful intrusion into one's private activities in such a manner as to outrage or cause mental suffering, shame or humiliation to a person of ordinary sensibilities." *Welling v. Weinfeld*, 866 N.E.2d 1051, 1053 (Ohio 2007) (quoting *Housh v. Peth*, 133 N.E.2d 340, 343 (Ohio 1956)). The plaintiff must have a "reasonable expectation of privacy" in the area or subject matter in which the alleged intrusion occurs. *Retuerto v. Berea Moving Storage & Logistics*, 38 N.E.3d 392, 406 (Ohio Ct. App. 2015) (internal quotation marks omitted). This expectation depends on the "totality of the circumstances." *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 761 (N.D. Ohio 2013).

In the present case, Luis alleges that he began exchanging electronic communications with Catherine in February 2009. Nothing in the complaint suggests that Luis or Catherine expected other people to monitor these communications, nor does Awareness contend that any other person had a legitimate reason to access these exchanges. In addition, the complaint specifically alleges that Luis's "conversations and communications were private," and that the installation of WebWatcher allowed Joseph and the other defendants to "intercept and record

conversations and actions to which they would not otherwise be privy." These allegations sufficiently establish that Luis had a reasonable expectation of privacy in his exchanges of electronic communications with Catherine. *Cf. Lazette*, 949 F. Supp. 2d at 761 (rejecting a motion to dismiss an intrusion claim in part because the emails at issue "were highly personal and private").

Luis next alleges that Awareness carried out the intrusion by intercepting his communications in violation of the federal and state Wiretap Acts. *See* Part II.D.1.a. above. Awareness's conduct was therefore "wrongful" for the purposes of Luis's intrusion claim. *See LeCrone v. Ohio Bell Tel. Co.*, 201 N.E.2d 533, 536 (Ohio Ct. App. 1963) (observing that the kind of conduct giving rise to an intrusion claim "generally would be criminal" or "a violation of public utility law"); *see also Retuerto*, 38 N.E.3d at 407 (noting that an example of conduct constituting intrusion "would be wiretapping").

Finally, Luis alleges that learning of Awareness's conduct caused him "surprise and dismay." He adds that, after intercepting his communications, Awareness disclosed "private and potentially embarrassing facts" to third parties such as Joseph. These allegations support a reasonable inference that Awareness's alleged intrusion caused "mental suffering, shame or humiliation." *See Welling*, 866 N.E.2d at 1053. Luis therefore adequately pleaded the last remaining aspect of his common-law intrusion claim. *Cf. LeCrone*, 201 N.E.2d at 536 ("As a general proposition, eavesdropping on phone conversations of another by unauthorized mechanical means, or a so[-]called 'tap,' is the kind of act or conduct that fits the definition of an intrusion or prying into another's private affairs.").

The district court reached the opposite conclusion. It held that Luis had failed to state a claim against Awareness because (1) Luis's factual allegations were too sparse, and (2) any liability should be attributed to Joseph rather than to Awareness.

We find the district court's analysis unconvincing. First, as described above, Luis alleged factual content related to each element of his intrusion claim. The complaint admittedly could contain additional details, and Luis's intrusion claim against Awareness may yet fail, but at this point Luis need nudge his claim past only the "speculative level." *See Bell Atl. Corp. v.*

Twombly, 550 U.S. 544, 555 (2007); *see also Bassett v. Nat'l Collegiate Athletic Ass'n*, 528 F.3d 426, 430 (6th Cir. 2008) ("*Twombly* does not require heightened fact pleading . . . ." (internal quotation marks omitted)). Luis, in other words, has provided enough information for a factfinder to reasonably infer that Awareness was responsible for each element of an intrusion claim. Luis's complaint is therefore adequate. *See Kreipke v. Wayne State Univ.*, 807 F.3d 768, 774 (6th Cir. 2015) (noting that a complaint should "contain either direct or inferential allegations respecting all material elements necessary for recovery under a viable legal theory" (internal quotation marks omitted)).

Second, Luis's intrusion claim does not depend on attributing the actions of Joseph to Awareness. Rather, as previously explained, Luis alleges that Awareness itself violated the federal and state Wiretap Acts by acquiring Luis's communications. Awareness is therefore unable to escape Luis's claims simply by arguing that a different party was actually more culpable. We accordingly conclude that Luis has adequately stated an intrusion claim against Awareness.

VI. CONCLUSION

Our holdings should not be construed as foreshadowing the ultimate outcome of Luis's claims. Awareness may yet prevail on summary judgment or at trial. For now, however, Luis's claims are sufficient to survive Awareness's motion to dismiss. The judgment of the district court is therefore **REVERSED** and the case is **REMANDED** for further proceedings consistent with this opinion.

DISSENT

ALICE M. BATCHELDER, Circuit Judge, dissenting. I agree that the complaint sufficiently alleges that WebWatcher "intercepts" communications within the meaning of the Wiretap Act, but my agreement with the majority ends there. Regarding his § 2511 claim, Luis's complaint does not allege that Awareness itself intercepted Luis's communications. As for § 2512, even assuming that Luis alleges a violation of that section, the Wiretap Act does not provide a private cause of action. I would affirm.

Luis's § 2511 argument on appeal is admittedly compelling: Awareness, by operating the online software central to WebWatcher's functionality, bears the same level of culpability as its customer for the software's illegal interceptions. But this theory of the case[1] is not alleged in the complaint. No matter how liberally we read Luis's complaint, he simply does not allege that Awareness was the one intentionally doing the intercepting.

The fact is that the complaint never names Awareness in the context of WebWatcher's operation. Awareness is named only twice. Initially, in paragraph 12, Awareness is identified as one of the defendants; that paragraph merely states that the company "is the maker of WebWatcher computer monitoring software . . . and is responsible for all marketing of this product." The only other mention is in paragraph 96 of the complaint's substantive allegations, which focuses on Awareness's marketing and design of WebWatcher.[2] The allegations include intentionally marketing WebWatcher to spouses, knowing that WebWatcher could be used surreptitiously, and knowing that it should have been modified to prevent any illegal use. The bulk of Luis's factual allegations describe the conduct of other defendants now dismissed from the suit.

---

[1]Luis's current theory of his case against Awareness is noticeably absent from his opposition to Awareness's motion to dismiss. It first appears in his objections to the magistrate judge's R&R. Inexplicably, Awareness did not raise the issue of waiver, thereby itself forfeiting an otherwise-sound basis for affirmance.

[2]Luis's opposition to Awareness's motion to dismiss also focuses on Awareness's actions in manufacturing, marketing, and selling WebWatcher.

The majority accepts Luis's argument on appeal that the complaint directly implicates Awareness in paragraph 77. But this reading is much more than just charitable—it grasps at straws. In describing how WebWatcher operates, Paragraph 77 uses only a possessive pronoun that lacks any antecedent: "WebWatcher immediately and *instantaneously* routs the intercepted communications to their servers located in California to be stored for their subscribers to later retrieve at their leisure." Awareness is neither named nor the subject of the action. This paragraph, located amidst Luis's allegations against the other defendants, does not give rise to the plausible inference that *Awareness* intentionally intercepted Luis's communications. *See Ashcroft v. Iqbal*, 556 U.S. 662, 682–83 (2009).

Even setting aside *Twombly* and *Iqbal*'s pleading standards (as the majority does), the main purpose of a complaint has always been "to 'give the defendant fair notice of what the claim is and the grounds upon which it rests.'" *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (quoting *Conley v. Gibson*, 355 U.S. 41, 47 (1957)). Luis's complaint fails even this lenient standard. It does not put Awareness on notice that it—the manufacturer and seller—could be liable for anonymous customer Joseph Zang's misuse of the WebWatcher. Luis's novel theory of liability does not appear even to have been tried, much less to have been successful, in any previous case. Neither Awareness nor the district court should have been expected to divine it from Luis's allegations against the other defendants. I would affirm the district court's dismissal of Luis's § 2511 claim against Awareness. I would affirm the dismissal of Luis's state-law claims for the same reason. *See Nix v. O'Malley*, 160 F.3d 343, 348 (6th Cir. 1998) (interpreting the Ohio Wiretap Act identically to the federal Wiretap Act).

As for Luis's § 2512 claim against Awareness, I am uncertain whether the complaint's factual allegations and the attached marketing materials plausibly indicate that the WebWatcher is "primarily useful for the purpose of the surreptitious interception of . . . electronic communications." *See* 18 U.S.C. § 2512(1)(b). A monitoring device like the WebWatcher is plainly useful for purposes wholly consistent with full disclosure, including an employer's monitoring of its employees or parental monitoring of children. But even accepting that Luis has alleged a violation of § 2512, the Wiretap Act lacks a private right of action to remedy that

violation. The majority's contrary conclusion distorts the statutory text and lacks any standard to guide future litigants.

The Wiretap Act, a criminal statute, contains a private right of action to remedy certain violations. The provision creating this right of action reads as follows:

> [A]ny person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity . . . which engaged in that violation such relief as may be appropriate.

§ 2520(a). The series of verbs "intercepted, disclosed, or . . . used" comes from § 2511(1)(a)–(e). There is no dispute that a plaintiff must be the victim of a § 2511 violation in order to sue under § 2520(a).

But who may be liable under this provision? As the majority correctly notes, the phrase "engaged in that violation" narrows the category of possible defendants. "[T]hat violation" plainly refers back to the earlier verb series; a proper defendant is one who "engaged in" an illegal "intercept[ion], disclos[ure], or . . . use[]." Every circuit court that has addressed the issue has so held. *See DirecTV, Inc. v. Treworgy*, 373 F.3d 1124, 1127 (11th Cir. 2004) (holding that § 2520(a) does not create a private right of action for possession of a device in violation of § 2512(1)(b), because the plain language limits the class of defendants to individuals or entities that committed the violation suffered by the plaintiff); *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 169 (5th Cir. 2000) (holding that § 2520(a) provides a right of action only against a defendant who "intercepted, disclosed, or used" the covered communications); *see also DirecTV Inc. v. Robson*, 420 F.3d 532, 538–39 (5th Cir. 2005) (noting that § 2520(a) does not provide a private right of action "for merely possessing or purchasing" a device in violation of § 2512(1)(b)); *DirecTV, Inc. v. Nicholas*, 403 F.3d 223, 227 (4th Cir. 2005) (quoting approvingly that court's earlier conclusion in *Flowers v. Tandy Corp.*, 773 F.2d 585, 589 (4th Cir. 1985), that "[t]he express language of § 2520 is . . . not susceptible to a construction which would provide a cause of action against one who manufactures or sells a device in violation of § 2512 but does not engage in conduct violative of § 2511").

Having come this far, the majority inexplicably fails to reach the only logical conclusion: a defendant who violates only § 2512—which criminalizes "mail[ing]," "manufactur[ing]," "sell[ing]," "assembl[ing]," "possess[ing]," and "advertis[ing]" devices "primarily useful for" such interception—faces no civil liability. Manufacture, marketing, and sale do not "engage[]" the manufacturer or seller in the subsequent use of the device by someone else.

The majority distinguishes *Treworgy* and *Robson*, which referred specifically to possession of a device, but it does not consider the other above-cited cases. *See Peavy*, 221 F.3d at 169 (rejecting liability for illegally procuring an illegal interception); *Flowers*, 773 F.2d at 589 (rejecting liability for illegal manufacture or sale). And the only supporting authority the majority can muster is an alternative holding from an out-of-circuit district court. *See DirecTV, Inc. v. Tasche*, 316 F. Supp. 2d 783, 789 (E.D. Wis. 2004) (adopting in the first instance a broad interpretation of § 2520 recognizing a private right of action for all Wiretap Act violations).

Nor does the majority cogently explain why manufacturing, marketing, and selling should be treated differently from possession. Instead of addressing these violations categorically, the majority dives into the facts of this case: Awareness took an "active role." This approach introduces two flaws.

As a factual matter, the opinion confuses Awareness's alleged violations of § 2512 with violations of § 2511. The majority says that Luis can sue Awareness for violating § 2512 because of Awareness's "active[] engage[ment] in the operation of WebWatcher by maintaining the servers" that stored intercepted communications. But that is exactly the activity that constitutes the violation of § 2511. It has nothing to do with intentionally "manufactur[ing], assembl[ing], possess[ing], or sell[ing] any" device, the activity prohibited by § 2512.

But even setting aside this confusion, the majority's nebulous, fact-based analysis is hardly a reasoned way to determine whether a cause of action exists. The majority's holding, if prescriptive, will result in case-by-case determinations of whether this or that defendant's actions rose to the level of "engagement" in a § 2511 violation. And although "engagement" is apparently broader than actually committing the violation, the majority's opinion gives no

guidance as to where the line is to be drawn. There is no reason to inject such indeterminacy into the start of every Wiretap Act lawsuit.

The simple alternative to this whole muddle is apparent from a straightforward reading of the statutory text. It has been adopted by every circuit to consider the issue until now. The plain meaning of § 2520(a) allows a plaintiff to recover only from a defendant who personally intercepted, disclosed, or used his communications in violation of § 2511.

I respectfully dissent.