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

File Name: 15a0253p.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

WILLIAM LONG, individually and on behalf of J.L.; BARBARA LONG, individually and on behalf of J.L.; JONATHAN LONG; MELISSA LONG,

Plaintiffs-Appellants,

v.

INSIGHT COMMUNICATIONS OF CENTRAL OHIO, LLC,

Defendant-Appellee.

No. 14-3996

Appeal from the United States District Court
for the Northern District of Ohio at Cleveland.
No. 1:14-cv-01096—Patricia A. Gaughan, District Judge.

Argued: June 17, 2015

Decided and Filed: October 23, 2015

Before: GUY, GIBBONS, and ROGERS, Circuit Judges.

COUNSEL

ARGUED: Matthew D. Greenwell, CHARLES V. LONGO, CO., L.P.A., Beachwood, Ohio, for Appellants. Jeffrey J. Jones, JONES DAY, Columbus, Ohio, for Appellee. **ON BRIEF:** Matthew D. Greenwell, CHARLES V. LONGO, CO., L.P.A., Beachwood, Ohio, for Appellants. Jeffrey J. Jones, Matthew J. Chisman, JONES DAY, Columbus, Ohio, for Appellee.

OPINION

RALPH B. GUY, JR., Circuit Judge. Plaintiffs appeal the dismissal of their claims against defendant Insight Communications of Central Ohio, d/b/a Time Warner Cable ("TWC"),

arising out of TWC's mistaken disclosure of plaintiffs' basic subscriber information in response to a grand jury subpoena. Reviewing the dismissal *de novo*, we find that plaintiffs failed to state a claim upon which relief may be granted either for violation of the Stored Communications Act ("SCA") (18 U.S.C. § 2707(a)), or for invasion of privacy, intentional disclosure of private information, intentional infliction of emotional distress, or breach of contract under Ohio law. Accordingly, the district court's judgment in favor of TWC is affirmed.

I.

Plaintiffs—William Long, Barbara Long, Jonathan Long, Melissa Long, and JL (a minor)—alleged that they resided at 14064 Chardon Windsor Road, Chardon, Ohio, in early 2012. At that time, TWC provided internet and cable services to plaintiffs' residence pursuant to a Subscriber Agreement and incorporated Privacy Notice. The pertinent allegations were accurately recounted by the district court as follows:

> On March 27, 2012, Special Agent Richard Warner of the Bureau of Criminal Investigation (BCI), Investigation Division in the Computer Crimes Unit, was conducting an online internet investigation to identify individuals possessing and sharing child pornography. An internet protocol address, known as an IP address, is a code of numbers that identifies a particular computer on the internet. Internet Service Providers (ISP), such as [TWC], assign their customers IP addresses. While conducting his investigation, Agent Warner located a suspect using a public IP address of 173.88.218.170 (the .170 address) and found several hundred images and movie files titled consistent with child pornography. The IP address of plaintiffs' computers at that time was 173.88.218.70 (the .70 address). [In other words, there was a difference of one digit between the two IP addresses.]
>
> Agent Warner downloaded the questionable material and determined that it was stored on the computer assigned the .170 address. On April 4, 2012, Agent Warner requested that [the] Geauga County Prosecutors' Office issue a Grand Jury subpoena requiring TWC to provide subscriber information for the .170 address. A subpoena was issued by the Prosecutors' Office and served on TWC requesting the information. TWC responded to the subpoena on April 11, 2012[,] and indicated that the .170 address was assigned to plaintiff Barbara Long. Based on this information, BCI obtained a search warrant for plaintiffs' residence. On April 20, 2012, BCI and local law enforcement personnel executed the search warrant on plaintiffs' residence. While searching the residence, the BCI agents determined that the IP address assigned to plaintiffs' TWC account was the .70 address and not the .170 address, as requested from TWC. The search was terminated and Agent Warner explained to plaintiffs that a mistake had been made

> by TWC. Agent Warner was later advised by TWC that it had "run the wrong IP address."

Long v. Insight Commc'ns of Cent. Ohio, LLC, No. 1:14-cv-1096, 2014 WL 4425738 at *1 (N.D. Ohio Sept. 8, 2014). Plaintiffs alleged that the search (which is not separately challenged here) was "extensive, destructive, and in plain sight of all of [their] neighbors." The search was terminated once the error was discovered, and no evidence of criminal activity was found.

Plaintiffs did not allege any defect with respect to the grand jury subpoena—only that TWC misidentified Barbara Long as the subscriber assigned the .170 IP address because TWC had "run the wrong IP address." Specifically, TWC was alleged to have disclosed Barbara Long's name, "home address, telephone numbers, and length of service." Without providing any further factual basis, plaintiffs asserted that "TWC's conduct was knowing, intentional, willful, wanton, malicious, and fraudulent."[1]

Plaintiffs' complaint alleged a federal claim for disclosure of their subscriber information without authorization in violation of the SCA (18 U.S.C. § 2707(a)) (Count I), and state-law claims for "Negligent Disclosure of Private Information," "Invasion of Privacy," "Intentional Infliction of Emotional Distress," and "Breach of Contract" (Counts II-V). TWC moved to dismiss these claims on a number of alternative grounds, including that the claims were barred under one or more defenses provided by the SCA; that TWC was protected by qualified privilege under Ohio common law; and that plaintiffs failed to state a claim on the merits under either the SCA or Ohio law. *See* FED. R. CIV. P. 12(b)(6).

The district court rejected TWC's claim of immunity under § 2703(e), but found that § 2707(e)'s "good faith reliance" defense barred all of plaintiffs' claims. *See* 18 U.S.C. §§ 2703(e) and 2707(e). The district court also concluded that the state-law claims failed on the merits because the factual allegations were insufficient to establish that TWC disclosed the information intentionally, wrongfully, or in breach of contract. *Long*, 2014 WL 4425738, at *3-4. Judgment was entered accordingly, and this appeal followed.

---

[1]Plaintiffs represented to the district court that the substance of their averments was unchanged by an amended complaint that was filed prior to removal but not made part of this record. Since plaintiffs have not suggested otherwise on appeal, we review the allegations that were before the district court.

II.

This court reviews a district court's dismissal for failure to state a claim *de novo*. *Courie v. Alcoa Wheel & Forged Prods.*, 577 F.3d 625, 629 (6th Cir. 2009). In doing so, we also may affirm the judgment on any ground supported by the record. *Wausau Underwriters Ins. Co. v. Vulcan Dev., Inc.*, 323 F.3d 396, 403-04 (6th Cir. 2003).

To survive a 12(b)(6) motion, the complaint must contain "enough facts to state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). In evaluating the complaint, the court must take the well-pleaded facts as true but is "'not bound to accept as true a legal conclusion couched as a factual allegation.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted). Indeed, although state of mind may be alleged generally, "the plaintiff still must plead facts about the defendant's mental state, which, accepted as true, make the state-of-mind-allegation 'plausible on its face.'" *Republic Bank & Trust Co. v. Bear Stearns & Co.*, 683 F.3d 239, 247 (6th Cir. 2012) (citation 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." *Iqbal*, 556 U.S. at 678; *see also 16630 Southfield Ltd., P'ship v. Flagstar Bank, F.S.B.*, 727 F.3d 502, 504 (6th Cir. 2013); *Estate of Barney v. PNC Bank, N.A.*, 714 F.3d 920, 924-25 (6th Cir. 2013).

III.

Title II of the Electronic Communications Privacy Act of 1986 (ECPA), commonly referred to as the Stored Communications Act (SCA) (codified as amended at 18 U.S.C. §§ 2701-2712), governs the various circumstances under which a service provider may divulge the contents of certain electronic communications or disclose other subscriber or customer records and information. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004) (outlining the structure of the SCA). This case, however, involves only the provisions governing a service

provider's disclosure of basic subscriber information to a governmental entity in response to a grand jury subpoena.[2]

A. Unauthorized Disclosure

The SCA dictates that—except as otherwise permitted—a service provider "shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity." 18 U.S.C. § 2702(a)(3). But, the exceptions that follow expressly permit a provider to divulge such records or information when, among other things, it is "otherwise authorized in section 2703." 18 U.S.C. § 2702(c)(1); *see also id.* at § 2702(c)(2)-(6) (other exceptions). As amended, § 2703 provides, in relevant part, that a governmental entity may require a service provider to disclose a subset of basic subscriber or customer information—including name, address, phone number, and length of service—"when the governmental entity uses [1] an administrative subpoena authorized by a Federal or State statute or [2] a Federal or State grand jury or trial subpoena[.]" 18 U.S.C. § 2703(c)(2) (as amended).

Reading these provisions together, and given that no defect was alleged with respect to the grand jury subpoena in this case, we assume that TWC would have been authorized to disclose the basic subscriber information associated with the .170 IP address in response to that subpoena. As plaintiffs alleged, however, TWC mistakenly disclosed the subscriber information associated with plaintiffs' .70 IP address instead. TWC's error was allegedly made in the course of retrieving the information to be disclosed (*i.e.*, "running the IP address"). Notably, plaintiffs have not alleged any facts (or argued that there are any facts) to suggest that TWC was aware of the error at the time of the disclosure. The district court found plaintiffs had alleged that "TWC made a mistake, a typographical error, in responding to the subpoena." *Long*, 2014 WL 4425738, at *3. Our *de novo* review of the complaint confirms that there are no facts from which we may infer that TWC's unauthorized disclosure of plaintiffs' information was the result of

[2]The parties do not dispute that TWC was a provider of an electronic communication service to the public within the meaning of the SCA. *See* 18 U.S.C. § 2711(1) ("'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications") (incorporating definition from 18 U.S.C. § 2510(15)). As such, it is immaterial whether TWC was also a provider of a remote computing service as defined in 18 U.S.C. § 2711(2). Also, it is evident that the Ohio BCI comes within the definition of a "governmental entity." *See* 18 U.S.C. § 2711(4) ("the term 'governmental entity' means a department or agency of the United States or any State or political subdivision thereof").

anything other than inadvertence or negligence. Accepting these well-pleaded facts as true, we turn to the question of whether plaintiffs have stated a plausible claim for relief under the SCA.

B. Dismissal

TWC raised three separate grounds for dismissal of this claim—any one of which may be a basis to affirm. Addressing TWC's defenses, the district court rejected the claim of immunity under § 2703(e) because TWC could not show that plaintiffs' information had been provided "in accordance with the terms of" a subpoena. 18 U.S.C. § 2703(e). But, explaining that similarly restrictive language was omitted from § 2707(e), the district court concluded that the "good faith reliance" defense was intended "to provide a defense where a provider responds to a subpoena with a good faith belief that it was acting pursuant to that subpoena although a mistake was made in so responding." *Long*, 2014 WL 4425738, at *3. In other words, TWC's inadvertent mistake would not negate its otherwise good faith reliance on the undisputedly valid grand jury subpoena. *Id*.[3]

Plaintiffs argue that the district court misinterpreted and misapplied the defense to bar the claims in this case. In particular, plaintiffs contend that "good faith reliance on" a "grand jury subpoena" should be interpreted to provide a defense *only* when a provider relied on a facially valid subpoena that was later claimed to have been invalid. Although several courts have recognized the defense in such a situation, none of those courts' decisions considered whether the defense should also apply when a provider makes a mistake in responding to a valid subpoena. *See, e.g.*, *Sams v. Yahoo! Inc.*, 713 F.3d 1175, 1180-81 (9th Cir. 2013); *McCready v. eBay, Inc.*, 453 F.3d 882, 891-92 (7th Cir. 2006); *Freedman v. Am. Online, Inc.*, 325 F. Supp. 2d 638, 647-50 (E.D. Va. 2004). We do not decide whether the district court properly interpreted or applied § 2707(e)(1), however, because TWC's mistaken disclosure of plaintiffs' subscriber information cannot state a plausible claim for relief under the SCA.[4]

---

[3]"A good faith reliance on . . . a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization . . . is a complete defense to any civil or criminal action[.]" 18 U.S.C. § 2707(e)(1); *see also* 18 U.S.C. § 2520(d)(1) (nearly identical defense under Title I of the ECPA).

[4]For this reason, we also do not decide which, if any, of the tests that have been articulated for determining "good faith reliance" would be appropriate in this case. *See Sams*, 713 F.3d at 1180 (rejecting the *Freedman* court's formulation); *Freedman*, 325 F. Supp. 2d at 647-48 (adopting test applied under 18 U.S.C. § 2520(d)(1)); *Frierson v. Goetz*, 99 F. App'x 649, 653 (6th Cir. 2004) (finding "good faith reliance" defense applied under 18 U.S.C.

C. Failure to State a Claim under the SCA

The SCA provides a civil cause of action for damages or other relief to any person "aggrieved by any violation of [the SCA] in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind[.]" 18 U.S.C. § 2707(a). As discussed, it would be a violation for a provider to "knowingly divulge" subscriber information if the disclosure is not otherwise permitted under the SCA. TWC argued for dismissal on the grounds that its mistaken disclosure of plaintiffs' information was insufficient to establish that it acted with the required state of mind. We agree.

We accept the allegation that TWC's error resulted in an unauthorized disclosure of plaintiffs' subscriber information to a governmental entity. But, no facts were alleged to suggest that TWC was aware of the error at the time of the disclosure, namely that the information it disclosed was not associated with the IP address that was the subject of the grand jury subpoena. Without arguing to the contrary, plaintiffs contend that it is sufficient to have alleged that TWC was aware of the "act" of disclosure. Tellingly, plaintiffs maintain that TWC may be held liable for negligently or recklessly failing to ensure the accuracy of the information it disclosed in response to the subpoena. Whether this would be sufficient to establish the requisite state of mind is a question of statutory interpretation that we review *de novo*. *See Elgharib v. Napolitano*, 600 F.3d 597, 601 (6th Cir. 2010). The inquiry begins with a natural reading of the full text, including the language and design of the statute as a whole; considers the common-law meaning of its terms; and may examine the relevant legislative history if the statutory language is not clear. *Id*.

Starting with the relevant language, plaintiffs must show that "the conduct constituting the violation"—here, that TWC "knowingly" divulged plaintiffs' subscriber information without authorization—was "engaged in with a knowing or intentional state of mind." The provisions governing disclosures of subscriber information to governmental entities make clear that not every disclosure is prohibited. The most natural reading of this language requires a showing that the provider knew not only that it was divulging information (*i.e.*, that the act of disclosure was

---

§ 2520(d)(1) where the defendant officer held "an honest and reasonable belief that he acted legally pursuant to a valid court order issued in accordance with state law").

not inadvertent), but also what information was being divulged (*i.e.*, the facts that made the disclosure unauthorized). *See McFadden v. United States*, 135 S. Ct. 2298, 2304 (2015) (holding that the most natural reading of 21 U.S.C. § 841(a)(1) is that "the word 'knowingly' applies not just to the statute's verbs but also to the object of those verbs"); *Morissette v. United States*, 342 U.S. 246, 270-71 (1952) (interpreting "knowingly converts" to require that defendant "had knowledge of the facts, though not necessarily the law, that made the taking a conversion"). The factual allegations do not permit an inference that TWC knew that the wrong subscriber information was being divulged in response to the subpoena.[5]

The terms "knowing" and "intentional" are not defined by the statute, and alone may have more than one meaning. But, in context, the language specifies that it is the conduct constituting the violation (not just the act of disclosure) that must have been knowing or intentional. Further, this interpretation is supported by the legislative history for the ECPA. First, although not specific to the SCA, the Senate Report explained that, "[a]s used in the [ECPA], the term 'intentional' is narrower than the dictionary definition . . . [and] means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective." S. Rep. 99-541, at 23 (1986) (*reprinted at* 1986 U.S.C.C.A.N. 3555, 3577); *see also* H. Rep. No. 99-647, at 48 (1986) (same). It is reasonable to conclude that this definition was intended to apply to both Title I and Title II of the ECPA.

Further, the legislative history includes the explanation that "a knowing state of mind is (1) an awareness of the nature of the conduct, (2) an awareness of or a firm belief in the existence of the circumstance, and (3) an awareness of or a firm belief in the substantial certainty of the result." H. Rep. 99-647, at 49. Also, in discussing the SCA's related prohibition on the disclosure of the contents of communications in § 2702(a), the legislative history specifically advises that: "The requirement that a violator must 'knowingly' divulge the contents is intended

[5]It is this mistake that distinguishes this case from *Freedman*, where the defendant knowingly divulged the plaintiffs' subscriber information in response to a warrant request but claimed to have been mistaken about the validity of the warrant. *See Freedman v. Am. Online, Inc.*, 329 F. Supp. 2d 745, 749 (E.D. Va. 2004) (clarifying *Freedman*, 325 F. Supp. 2d at 645). This case does not involve a mistake as to the legal validity of the disclosure, but a lack of knowledge about the fact that the wrong information was being divulged. *See, e.g.*, *United States v. Wuliger*, 981 F.2d 1497, 1502-03 (6th Cir. 1992) (knowledge under 18 U.S.C. § 2511 included the fact of whether the interception was nonconsensual).

to make clear that 'reckless' or 'negligent' conduct is not sufficient to constitute a violation of this section." S. Rep. 99-541, at 36-37; *see also* H. Rep. 99-647, at 64 ("The concept of 'knowingly' does not include, however, 'reckless' or 'negligent' conduct."). This supports our interpretation that for the conduct constituting the violation to have been knowing and intentional, TWC must have known that it was not divulging the subscriber information associated with the IP address that was the subject of the subpoena. The dismissal of the claim for violation of the SCA is affirmed.

IV.

Finally, plaintiffs argue that the district court erred in concluding, in the alternative, that the claims asserted under Ohio law failed on the merits. Reviewing the dismissal of these claims *de novo*, plaintiffs have not demonstrated error.

Count II. Plaintiffs did not dispute that there is not a recognized cause of action for "Negligent Disclosure of Private Information" under Ohio law, but argued that this count was meant to assert a claim of intentional disclosure in violation of Ohio Rev. Code § 1347.10. The district court found that this claim failed because plaintiffs had not pleaded facts sufficient to allege an intentional disclosure. More fundamentally, however, this claim fails because the statute governs personal information maintained in a "personal information system," which is defined as a collection of related records that are "maintained by a state or local agency." OHIO REV. CODE §§ 1347.01 and 1347.10. This is plainly not the case here.

Counts III and IV. Dismissal of the claims for "Invasion of Privacy" and "Intentional Infliction of Emotional Distress" was not error. The invasion of privacy plaintiffs assert is "the 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." *Housh v. Peth*, 133 N.E.2d 340, 341 (Ohio 1956) (syllabus 2). However, negligent intrusion into one's private activities does not constitute an actionable invasion of privacy. *See McCormick v. Haley*, 307 N.E.2d 34, 38 (Ohio Ct. App. 1973). Nor do the allegations of TWC's mistaken disclosure of plaintiffs' information plausibly allege that defendant acted with the necessary intent to inflict emotional distress required to state a claim for intentional infliction of emotional distress under Ohio law. *See Burkes v. Stidham*, 668 N.E.2d 982, 989 (Ohio Ct. App. 1995).

Count V. Plaintiffs argue that it was error to dismiss the breach of contract claim, which alleged that TWC violated the terms of its Subscriber Agreement and incorporated Privacy Notice by mistakenly disclosing plaintiffs' subscriber information in response to the grand jury subpoena. The district court did not err in dismissing this claim because the contract explained that the ECPA allows personally identifiable information to be obtained by governmental entities in some circumstances, including through the use of a subpoena, and gave TWC the authority to "comply with legal process when we believe in our discretion that we are required to do so." There were no facts to suggest that TWC did not believe it was responding to the subpoena when it mistakenly disclosed plaintiffs' subscriber information.

AFFIRMED.