FILED
United States Court of Appeals
Tenth Circuit

June 29, 2009

Elisabeth A. Shumaker
Clerk of Court

PUBLISH

UNITED STATES COURT OF APPEALS

TENTH CIRCUIT

FEDERAL TRADE COMMISSION,

Plaintiff - Appellee,

v.

ACCUSEARCH INC., d/b/a Abika.com; JAY PATEL,

Defendants - Appellants,

_____

JENNIFER STODDART, Privacy Commissioner of Canada,

Amicus Curiae.

No. 08-8003

APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF WYOMING (D.C. NO. 2:06-CV-00105-WFD)

Deborah L. Roden (Gay Woodhouse with her on the briefs) of Gay Woodhouse Law Office, P.C., Cheyenne, Wyoming, for Defendants - Appellants.

Lawrence DeMille-Wagman, Attorney, Federal Trade Commission, Washington, D.C., (William Blumenthal, General Counsel, John F. Daly, Deputy General Counsel for Litigation, Federal Trade Commission, Washington, D.C.; and Tracy S. Thorleifson, Kial S. Young, Federal Trade Commission, Seattle, Washington, with her on the brief), for Plaintiff - Appellee.

Edward R. McNicholas, Sidley Austin LLP, Washington, DC, filed an amicus curiae brief for Jennifer Stoddart, Privacy Commissioner of Canada, in support of Plaintiff - Appellee.

Before **HARTZ**, **TYMKOVICH**, and **HOLMES**, Circuit Judges.

HARTZ, Circuit Judge.

Abika.com is a website that has sold various personal data, including telephone records. The Federal Trade Commission (FTC) brought suit against the operator of the website, Accusearch Inc., and its president and owner, Jay Patel (collectively, Accusearch), to curtail Accusearch's sale of confidential information and to require it to disgorge its profits from the sale of information in telephone records. The FTC alleged that Accusearch's trade in telephone records (which are protected from disclosure under § 702 of the Telecommunications Act of 1996, 47 U.S.C. § 222 (2006)) constituted an unfair practice in violation of § 5(a) of the Federal Trade Commission Act (FTCA), 15 U.S.C. § 45(a) (2006). The district court granted the FTC summary judgment, *see FTC v. Accusearch, Inc.*, No. 06-CV-105-D, 2007 WL 4356786, at *10 (D. Wyo. Sept. 28, 2007), and after further briefing entered an injunction restricting Accusearch's future trade in telephone records and other personal information.

On appeal Accusearch contends that (1) the FTC's unfair-practice claim should have been dismissed because Accusearch broke no law and because the FTC had no authority to enforce the Telecommunications Act; (2) it was immunized from suit by the protections provided websites in the Communications

Decency Act (CDA), 47 U.S.C. § 230 (2006); and (3) the injunction is unnecessary to prevent it from resuming trade in telephone records and is unconstitutionally overbroad. Exercising jurisdiction under 28 U.S.C. § 1291, we reject each of Accusearch's contentions and affirm. First, conduct may constitute an unfair practice under § 5(a) of the FTCA even if it is not otherwise unlawful, and the FTC may pursue an unfair practice even if the practice is facilitated by violations of a law not administered by the FTC, such as the Telecommunications Act. Second, Accusearch's claimed defense under the CDA fails because it acted as an "information content provider" (and thus is not entitled to immunity) with respect to the information that subjected it to liability under the FTCA. *See* 47 U.S.C. § 230(f)(3). Finally, the injunction was proper despite Accusearch's prior halt to its unfair practices and the possibility that the resumption of those practices would be criminally prosecuted; and Accusearch waived in district court its claim on appeal that the injunction is overbroad.

I. BACKGROUND

A. Abika.com

Although the parties characterize the Abika.com website differently, they do not dispute the essential aspects of its operation. Any person interested in Abika.com's services could access the website through a search engine or by typing its address into an Internet browser. A visitor to the website would first see its homepage, which displayed various categories of information that could be

searched. The record contains one printout of the website from December 20, 2006, and one from November 27, 2007. The printouts show that some searches advertised on the homepage targeted information generally contained in government records, such as "court dockets," "sex offender records," and "Tax . . . Liens." Aplts. App., Vol. 4 at 1313; *id.* Vol. 5 at 1429. Other search categories related to intimate personal information, such as "Romantic Preferences," "Personality traits," and "Rumors." *Id.* Vol. 4 at 1313; *id.* Vol. 5 at 1429.

Accusearch stresses on appeal that the search services offered on Abika.com were primarily services provided by third-party researchers, who were required by Accusearch to provide assurances that they would perform their work in accordance with applicable law. The researchers had no direct contact with Abika.com's customers. As Accusearch explains, "all information passed between [customer] and researcher went through Abika.com, as an intermediary." Aplts. Reply Br. at 3. In placing a search order, a customer paid Accusearch an "administrative search fee," Aplts. App., Vol. 4 at 1246, and selected the type of

could know that a third-party researcher was involved in a transaction only by reading boilerplate contained on the website and in Accusearch's email correspondence. And even then, the customer was not provided contact information for any researcher.

B. Provision of Telephone Records

From February 2003 to January 2006 the Abika.com website advertised access to personal telephone records. The website stated that its customers could acquire "details of incoming or outgoing calls from any phone number, prepaid calling card or Internet Phone," and that "Phone searchers are available for every country of the world." *Id.* Vol. 4 at 1246–47 (internal quotation marks omitted). Abika.com's customers could purchase both cellphone and landline records. The website specified that cellphone records would detail the numbers dialed from a particular cellphone and generally include the "date, time and duration of the calls" made. *Id.* Vol. 2 at 475. Landline records would include the same information, save for the specific time at which calls were made.

Acquisition of this information would almost inevitably require someone to violate the Telecommunications Act or to circumvent it by fraud or theft. The Act forbids telecommunications carriers from disclosing telephone records absent customer consent or the applicability of one of several exceptions. *See* 47 U.S.C. § 222(c)–(d). The Act provides as follows:

> Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

Id. § 222(c)(1). (We note the additional exceptions below.[1]) There is no dispute that the telephone records available on Abika.com constituted "individually identifiable customer proprietary network information" within the meaning of § 222,[2] or, more generally, that the Telecommunications Act barred disclosure of those records by telecommunications carriers. Although Accusearch (remarkably, in our view) maintained that it relied in good faith on its researchers' commitment to obey the law in acquiring information, it represented that it ceased offering

---

[1] The Act does not forbid telecommunications carriers from disclosing telephone records to (1) "initiate, render, bill, and collect for telecommunications services"; (2) protect telecommunications carriers and customers from the "fraudulent, abusive, or unlawful use of, or subscription to," telecommunications services; (3) provide certain "telemarketing, referral, or administrative services to the customer"; and (4) "provide call location information" to (a) public-safety personnel responding to a user's call, (b) legal guardians and family members in emergency situations involving "risk of death or serious physical harm," and (c) "providers of information or database management services" used to assist in the provision of emergency services. 47 U.S.C. § 222(d).

[2] "Customer proprietary network information" is defined to include "information contained in bills" and "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer." 47 U.S.C. § 222(h)(1).

telephone records in January 2006 after learning that a subsidiary of one of its researchers possibly obtained telephone data fraudulently.

C. Procedural History

The FTC filed suit against Accusearch on May 1, 2006, roughly four months after Accusearch ceased to offer telephone records. The complaint alleged that telephone records are protected against disclosure by the Telecommunications Act and that trade in such records constitutes an unfair practice in violation of § 5(a) of the FTCA, 15 U.S.C. § 45(a). Accusearch responded with a motion to dismiss, contending that the complaint failed to state a claim because the Telecommunications Act applies only to telephone carriers and because selling confidential telephone records was not otherwise unlawful. The district court denied the motion and Accusearch filed an answer. After conducting discovery the parties each moved for summary judgment.

The FTC argued that Accusearch's practices were unfair under the FTCA as a matter of law. Accusearch countered that it was immunized by the CDA, which, broadly speaking, protects Internet services from liability as publishers with respect to content provided by others. *See* 47 U.S.C. § 230(c). Accusearch contended that it was entitled to this immunity because the FTC's claim treated it as the publisher of telephone records that were provided by others (that is, telephone companies and independent researchers) and traded over Abika.com. The district court granted the FTC's motion and rejected Accusearch's assertion of

immunity. The court ruled that the FTC had established each element of its unfair-practice claim. And it concluded that Accusearch was not entitled to statutory immunity because it had "participated in the creation or development" of the information delivered to customers, *Accusearch*, 2007 WL 4356786, at *6 (brackets and internal quotation marks omitted), and because the FTC's claim did not "treat" Accusearch as a mere publisher of those records, *id*. at *5 (internal quotation marks omitted). It found that Accusearch's "claim of blissful ignorance [of its researchers' misconduct] is simply not plausible in light of the facts of this case," *id.* at *7, explaining that "[e]ven if [Accusearch was] unaware at the outset how these records were obtained, emails documenting the ordering process

because it voluntarily ceased dealing in telephone records before the FTC filed its complaint, and because resumption of those activities would subject it to newly enacted criminal sanctions regardless of the injunction. Accusearch further asserts that the injunction improperly restricts its ability to deal in consumer data other than telephone records. This overbreadth, we are told, violates Accusearch's due-process, free-speech, and equal-protection rights.

II. DISCUSSION

A. Unfair-Practice Claim

The FTCA prohibits "unfair or deceptive acts or practices in or affecting commerce," 15 U.S.C. § 45(a)(1), and vests the FTC with authority to prevent such practices by issuing cease-and-desist orders, *id*. § 45(b), by prescribing rules, *id*. § 57a(a)(1)(B), and by seeking injunctive relief in federal district court, *id*. § 53(b). To be "unfair," a practice must be one that "[1] causes or is likely to cause substantial injury to consumers [2] which is not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition." *Id.* § 45(n).

The FTC argued below that Accusearch's practice of offering consumer telephone records over the Internet satisfied all three requirements. First, the FTC contended that substantial injury was caused by the subversion of the Telecommunications Act; it argued that consumers whose telephone records were obtained through Abika.com suffered emotional harm (sometimes from being

[3] After Accusearch ceased offering telephone records, Congress enacted the Telephone Records and Privacy Protection Act of 2006, which criminalizes the sale and receipt of confidential telephone records. *See* 18 U.S.C. § 1039.

Trade Commission Act, seeking to enjoin an unfair practice affecting commerce. *See id.* § 45(a) (declaring unfair practices unlawful); *id*. at § 53(b) (giving the FTC authority to seek enjoinment of unfair practices in federal district court). As set out above, the Telecommunications Act was relevant to that claim. But the complaint does not allege that Accusearch violated that Act. In any event, the FTC may proceed against unfair practices even if those practices violate some other statute that the FTC lacks authority to administer. *See Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 983 (D.C. Cir. 1985) (certain creditor remedies, which violated laws in a number of states, also unfair under § 5(a)). Indeed, condemnation of a practice in criminal or civil statutes may well mark that practice as "unfair." *See FTC v. R.F. Keppel & Bro.*, 291 U.S. 304, 313 (1934); *Am. Fin. Servs. Ass'n*, 767 F.2d at 983. By the same token, a practice, such as Accusearch's, which either encourages such condemned conduct or encourages the use of fraud or theft to circumvent the statute, may likewise be considered "unfair."

B. Immunity Under the Communications Decency Act

Accusearch's primary argument on appeal is that even if the FTC stated a claim, it is immune from liability under § 230(c)(1) of the CDA. *See* 47 U.S.C. § 230(c)(1). The CDA is intended to facilitate the use and development of the Internet by providing certain services an immunity from civil liability arising from content provided by others. *See Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330–31

(4th Cir. 1997). The prototypical service qualifying for this statutory immunity is an online messaging board (or bulletin board) on which Internet subscribers post comments and respond to comments posted by others. *See id.* at 328–29, 332 (discussing operation of messaging board and holding that it was "clearly protected by § 230's immunity"). Indeed, Congress enacted the CDA in response to a state-court decision, *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710, *5 (N.Y. Sup. Ct. May 24, 1995), which held that the provider of an online messaging board could be liable for defamatory statements posted by third-party users of the board. *See Fair Hous. Council v. Roommates.com, LLC*, 521 F.3d 1157, 1163 (9th Cir. 2008) (en banc) (noting Congress's concern about *Stratton Oakmont*). The *Stratton Oakmont* court ruled that the administrator of the board became a "publisher" when it deleted some distasteful third-party postings, and thus was subject to publisher's liability for the defamatory postings it failed to remove. 1995 WL 323710, at *4–5. The decision was criticized for discouraging the voluntary filtration of Internet content, because a forum provider's efforts to sanitize content would trigger liability that could be avoided by doing nothing. *See Roommates.com*, 521 F.3d at 1163.

The CDA, however, does more than just overrule *Stratton Oakmont*. To understand the full reach of the statute, we will need to examine some of the technical terms used in the CDA. But to put those terms in context we first quote the operative provisions of the law. Section 230(c)(1) provides as follows:

> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

Section 230(c)(2), which protects services that filter content, states:

> No provider or user of an interactive computer service shall be held liable on account of—
>
> > (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
> >
> > (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1). ["paragraph (1)" should probably be "subparagraph (A)," *see*

Accusearch essentially concedes the factual premise of the FTC's argument— namely, the absence of direct interaction among users of the Abika.com website. Although Accusearch occasionally tries to portray its website as an interactive forum on which independent researchers connected with persons seeking information, it ultimately acknowledges that "all information passed between the [customer] and researcher went through Abika.com, as an intermediary." Aplts. Reply Br. at 3.

But despite the FTC's accurate characterization of Abika.com, its interactivity argument does not fully respect the CDA's text. Section 230(f)(2) does not say that an interactive computer service must facilitate interaction among third parties; rather, it says that an interactive computer service is one that "provides or enables computer access by multiple users *to a computer server*." 47 U.S.C. § 230(f)(2) (emphasis added). *See Universal Commc'ns Sys., Inc. v. Lycos, Inc.*, 478 F.3d 413, 419 (1st Cir. 2007) ("web site operators . . . are providers of interactive computer services" because "[a] web site . . . enables computer access by multiple users to a computer server, namely, the server that hosts the web site." (internal quotation marks omitted)); *Batzel v. Smith*, 333 F.3d 1018, 1030 (9th Cir. 2003) (suggesting, but not deciding, that a website necessarily provides an interactive computer service). Accordingly, we are reluctant to embrace the FTC's contention that one who operates a website does not thereby provide an interactive computer service unless it allows interaction

among the users. Because we can resolve the matter of CDA immunity in this case without deciding whether the FTC's contention is correct, we leave it to another day.

information content provider." 47 U.S.C. § 230(c)(1). Thus, an interactive computer service that is also an "information content provider" of certain content is not immune from liability arising from publication of that content. *See Roommates.com*, 521 F.3d at 1162; *Ben Ezra, Weinstein, & Co., Inc. v. Am. Online Inc.*, 206 F.3d 980, 985 n.4 (10th Cir. 2000).

The CDA defines the term *information content provider* as "any person or

noting that *develop* can mean to "[m]ake something new" and "[c]ome into existence." Aplts. Am. Br. at 39 (internal quotation marks omitted). Because the information provided to its customers came originally from the telecommunications carriers, it argues, it made nothing new nor brought anything into existence. But the CDA uses the phrase "creation or development of information," 47 U.S.C. § 230(f)(3), and if the meaning of the word *develop* were limited to the two senses relied upon by Accusearch, the word *development* would add nothing not already conveyed by the word *creation*. "Under a long-standing canon of statutory interpretation, one should avoid construing a statute so as to render statutory language superfluous." *McCloy v. U.S. Dept. of Agric.*, 351 F.3d 447, 451 (10th Cir. 2003); *see Roommates.com*, 521 F.3d at 1168. We therefore examine whether we can reasonably construe *development* more broadly.

We can. When faced with an undefined statutory term, an investigation of its "core meaning" can be illuminating. *United States v. Montgomery*, 468 F.3d 715, 720 (10th Cir. 2006); *see also Muscarello v. United States*, 524 U.S. 125, 128–29 (1998) (investigating etymological origins of "carries" to uncover its "primary meaning"). The word *develop* derives from the Old French *desveloper*, which means, in essence, to unwrap. Webster's Third New International Dictionary 618 (2002) (explaining that *desveloper* is composed of the word *veloper*, meaning "to wrap up," and the negative prefix *des*). The dictionary definitions for *develop* correspondingly revolve around the act of drawing

something out, making it "visible," "active," or "usable." *Id*. Thus, a photograph is developed by chemical processes exposing a latent image. *See id*. Land is developed by harnessing its untapped potential for building or for extracting resources. *See id*. Likewise, when confidential telephone information was exposed to public view through Abika.com, that information was "developed." *See id.* (one definition of *develop* is "to make actually available or usable (something previously only potentially available or usable)").

This conclusion, however, does not end the inquiry. The question remains whether Accusearch was "'responsible, in whole or in part, for the . . . development of' the offending content." *Roommates.com*, 521 F.3d at 1162 (quoting § 230(f)(3)). That is, was it responsible for the development of the specific content that was the source of the alleged liability? The answer is "yes."

Just as the CDA does not define *development*, it does not define *responsible*. We need not provide a complete definition of the term that will apply in all contexts; but we can say enough to resolve this case and to assuage concern that the broad meaning for *development* that we have adopted will undermine the purpose of immunity under the CDA.

The meaning of *responsible* becomes an issue under the CDA when a court is considering whether CDA immunity from liability is unavailable because one is "responsible, in whole or in part, for the creation or development of information" that is the source of the liability. In this context—responsibility for harm—the

(b). We therefore conclude that a service provider is "responsible" for the development of offensive content only if it in some way specifically encourages development of what is offensive about the content.

In the case before us, the offending content was the disclosed confidential information itself. We need not construe the word *responsible* to extend beyond its core meaning in this context to conclude that Accusearch was responsible for the development of that content—for the conversion of the legally protected records from confidential material to publicly exposed information. Accusearch solicited requests for such confidential information and then paid researchers to obtain it. It knowingly sought to transform virtually unknown information into a publicly available commodity. And as the district court found and the record shows, Accusearch knew that its researchers were obtaining the information through fraud or other illegality.

Accusearch argues that our decision in *Ben Ezra*, 206 F.3d 980, establishes

because Id

"Plaintiff has not demonstrated [that America Online] worked so closely with [the third-party vendor] regarding the allegedly inaccurate stock information that [it] became an information content provider." *Id*. at 985. Accusearch argues that because America Online was not considered an information content provider despite soliciting the relevant information for online publication, Accusearch's own solicitation of information could not make it an information content provider either. But Accusearch takes too broad a view of what was the relevant information in *Ben Ezra*. Although America Online solicited stock quotations, the plaintiff's claim was based on *inaccuracies* in the solicited quotations. *See id.* at 983. The "offending content" was thus erroneous stock quotations and, unsurprisingly, America Online did not solicit the errors; indeed, it sent the vendor emails requesting that it "correct the allegedly inaccurate information."

responsible for the development of discriminatory preferences contained in its users' personal-profile pages. *Roommates.com*, 521 F.3d at 1167–68. Subscribers of the website were required to specify from a set of preselected answer choices their "sex, sexual orientation and whether [they] would bring children to a household." *Id*. at 1161; *see id.* at 1165 & n.17. Subscribers also had to select their "preferences in roommates with respect to the same three criteria." *Id*. at 1161. For example, subscribers seeking housing had to state "whether they [were] willing to live with 'Straight or gay' males, only with 'Straight' males, only with 'Gay' males or with 'No males.'" *Id*. at 1165. These preferences were then posted on a subscriber's profile page, where they could be reviewed by other subscribers looking for a roommate match. *Id*. To be sure, the matching service did not place discriminatory preferences in the minds of its users. It did not, in other words, create those preferences. But the court found that by requiring its users to disclose their illicit preferences, the service provider became "much more than a passive transmitter of information provided by others; it bec[ame] the developer, at least in part, of that information." *Id*. at 1166. It summarized: "[A] website helps to develop unlawful content, and thus falls within the exception to section 230, if it contributes materially to the alleged illegality of the conduct." *Id*. at 1168.

That language applies to Accusearch's role in this case. By paying its researchers to acquire telephone records, knowing that the confidentiality of the records was protected by law, it contributed mightily to the unlawful conduct of its

researchers. Indeed, Accusearch's responsibility is more pronounced than that of Roommates.com. Roommates.com may have encouraged users to post offending content; but the offensive postings were Accusearch's *raison d'etre* and it affirmatively solicited them.

An earlier Ninth Circuit case, *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119 (9th Cir. 2003), provides a useful comparison. In that case an unknown person created a bawdy dating profile for actress Christianne Carafano on the defendant's online-dating website. *See id.* at 1121. To create the profile, the anonymous poster had to draft an essay and "select answers to more than fifty questions from menus providing between four and nineteen options." *Id.* Some options were "sexually suggestive" and some were "innocuous." *Id.* The Ninth Circuit held that the dating service was not an information content provider of the libelous profile. *Id.* at 1124. As the en banc court would later explain in *Roommates.com*, "[t]he salient fact in *Carafano* was that the website's classifications of user characteristics did absolutely nothing to enhance the defamatory sting of the message, to encourage defamation or to make defamation easier." *Roommates.com*, 521 F.3d at 1172. Although an unknown person created Ms. Carafano's profile in part from preselected answer choices, the menus provided by the website did not encourage a defamatory response. *See id.* at 1171. Unlike Roommates.com, which prompted the disclosure of discriminatory preferences, the dating website provided only "neutral tools" which were

employed to create the offending content. *Id*. at 1172; *see Universal Commc'n Sys.*, 478 F.3d at 420 (messaging board immune with respect to posts it did not prompt);

Accusearch, 2007 WL 4356786, at *9. Accordingly, the injunction prohibits Accusearch from doing, among other things, the following:

court may consider "all the circumstances," including the "bona fides of the expressed intent to comply, the effectiveness of the discontinuance and, in some cases, the character of the past violations." *Id.* We review the decision to grant a permanent injunction for abuse of discretion. *John Allan Co. v. Craig Allen Co. L.L.C.*, 540 F.3d 1133, 1142 (10th Cir. 2008). The district court's discretion in this context is "necessarily broad and a strong showing of abuse must be made to reverse it." *W. T. Grant Co.*, 345 U.S. at 633.

Accusearch has not persuaded us that the district court abused its discretion. True, Accusearch ceased offering telephone records before litigation commenced. But, as the district court noted, because Accusearch remained in the "information brokerage business" it had the capacity to "engag[e] in similar unfair acts or practices" in the future. *Accusearch*, 2007 WL 4356786, at *9; *see also W.T. Grant Co.*, 345 U.S. at 633 ("effectiveness of the discontinuance" is a factor in assessing likelihood of recurrence). In Accusearch's view it has proved the absence of any need for prospective relief by expressing a willingness to disgorge nearly $200,000 in ill-gotten profits. But a district court is best situated to judge the sincerity of a litigant's contrition, *see W.T. Grant Co.*, 345 U.S. at 634, and Accusearch has given us no ground to second-guess the district court's judgment. *See United States v. Or. State Med. Soc.*, 343 U.S. 326, 333 (1952) (courts must "beware of efforts to defeat injunctive relief by protestations of repentance and reform").

burdensome than proving a criminal violation. For example, to violate § 1039 one must act "knowingly and intentionally." *Id.* § 1039(a)–(c). The injunction, on the other hand, imposes no scienter requirement and the law does not necessarily imply one. *See FTC v. Freecom Commc'ns, Inc.*, 401 F.3d 1192, 1204 n.7 (10th Cir. 2005) ("FTC need not prove scienter . . . to establish a § 5 violation."); 11A Charles Alan Wright, Arthur R. Miller & Mary Kay Kane, Federal Practice and Procedure § 2960, at 382 (2d ed. 1995) ("[A] violation of [a] decree need not be willful for a party to be held in civil contempt."). And a violation need not be proved to a jury beyond a reasonable doubt. *See* Charles Alan Wright, *supra* § 2960, at 379–80 (there is no constitutional right to a jury in civil-contempt proceedings and the contempt must be shown only by clear and convincing evidence, not beyond a reasonable doubt). The district court did not impose an inconsequential injunction. Thus, Accusearch's argument fails on its own terms.

In any event, "Congress . . . has power to provide for civil injunctive relief against activities which adversely affect interstate commerce, and that power extends to activities which are made criminal by state or federal law." *United States v. Cappetto*, 502 F.2d 1351, 1356 (7th Cir. 1974) (upholding injunction against gambling activities issued under the Organized Crime Control Act of 1970, which also made those activities a crime); *accord Nat'l Ass'n of Letter Carriers*, 470 F.2d at 271 (injunction against criminalized conduct proper in part because it was authorized by statutes "purely civil in nature"). In enacting the FTCA,

Congress gave the FTC express authority to seek permanent injunctive relief in federal court to prevent violations of § 5(a). *See* 15 U.S.C. §53(b); *FTC v. Kuykendall*, 371 F.3d 745, 749, 764 (10th Cir. 2004) (en banc).

In sum, the enactment of § 1039 does not undermine the propriety of the injunction against Accusearch.

2. Breadth of the Injunction

Although the district court determined only that Accusearch's trade in telephone records was unfair within the meaning of the FTCA, it issued an injunction restricting Accusearch's trade in "any individually identifiable information concerning a consumer." Aplts. App., Vol. 5 at 1606. Accusearch argues that the injunction should have been limited to its trade in telephone records, the specific practice found to be unlawful. *See FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 394–95 (1965) (FTC may "fence in" offenders by enjoining more than the specific misconduct previously engaged in, but the injunction must bear a "reasonable relation to the unlawful practices found to exist."). According to Accusearch, this overbreadth violates its due-process, free-speech, and equal-protection rights. (Because Accusearch's discussion of equal protection does not reference any particular feature of the injunction, we presume that the claim is tied to the only feature that Accusearch challenges on appeal—namely, its coverage of information other than telephone records.)

Accusearch, however, not only failed to preserve this claim of error below, it invited the alleged error. After the district court granted the FTC summary judgment, the parties submitted briefs on the propriety and scope of injunctive relief. Accusearch argued that an injunction was unnecessary and that, if the court disagreed, injunctive relief should be limited in certain respects. In connection with this alternate argument, Accusearch submitted a proposed injunctive order that had been "negotiated" with the FTC. Aplts. App., Vol. 5 at 1409. The proposed injunction set forth agreed-upon language and denoted several areas in which the parties could not reach consensus. Among the agreed-upon provisions were Section II, entitled "Prohibited Business Activities," which bars dealings in "consumer personal information," and the definition of that term as "any individually identifiable information concerning a consumer." *FTC v. Accusearch, Inc.*, No. 06-CV-105-D (Defs. Br. on Injunctive Relief, Ex. A at 2–5, Nov. 19, 2007).

Curiously, Accusearch submitted the proposed injunction as an attachment to a district-court brief in which it argued that the injunctive relief sought by the FTC would be overbroad because it was not limited to telephone records but covered "*all* consumer information." Aplts. App., Vol. 5 at 1411. That is, Accusearch appeared to object to provisions to which it had stipulated, perhaps indicating a clerical error or a drafting oversight. The FTC's responding brief took note of this inconsistency and reminded Accusearch that it had specifically

agreed to those provisions extending the injunction's coverage beyond telephone records. In reply, Accusearch made no effort to clarify its position or retract any

08-8003, *F.T.C. v. Accusearch Inc. DBA Abika.com & Jay Patel*

Tymkovich, J., concurring.

I write separately to emphasize what I see as an unnecessary extension of the CDA's terms "responsible" and "development," thereby widening the scope of what constitutes an "information content provider" with respect to particular information under the Act. *See* 47 U.S.C. § 230(c)(1), (f)(3).

The majority holds that by soliciting third-parties to obtain and then exposing the confidential telephone records to public view, Accusearch is *responsible*—at least in part—for *developing* that information. Under this definition, the line between passive posting of tortious or unlawful commentary, news articles, or other previously unpublished information and content development depends on an amorphous analysis of the motivations of the content provider in soliciting or acquiring that information. In the majority's view, a content provider seeking out the information in good faith may be able to obtain CDA immunity for any subsequent liability, as it would not have been "responsible, in whole or in part, for the . . . development of [that] information." § 230(f)(3). If the provider's motivations are not in good faith, however, the majority's approach transforms the provider into a developer of that information. The provider would then be deemed the information content provider for that information and lose its entitlement to CDA immunity. Instead of embarking on this path, I would avoid the need to interpret the CDA in the first instance.

I agree with the majority that Accusearch violated the FTCA, though I reach this conclusion because I believe the FTC sought and ultimately held Accusearch liable for its *conduct* rather than for the *content* of the information it was offering on the Abika.com website. Section 230 only immunizes publishers or speakers for the *content* of the information from other providers that they make public. § 230(c)(1) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."). The CDA says nothing about immunizing publishers or speakers for their own conduct in *acquiring* the information. Indeed, other courts have explicitly recognized this distinction. *E.g.*, *800-JR Cigar, Inc. v. GoTo.com, Inc.*, 437 F. Supp. 2d 273, 295 (D.N.J. 2006) ("[I]mmunity under the Act applies to any cause of action that would make service providers liable for information originating with a third-party user of the service. Immunity does not seem to fit here because the alleged fraud is the use of the trademark name in the bidding process, and not solely the information from third parties that appears on the search results page. It is not the purpose of the Act to shield entities from claims of fraud and abuse arising from their own pay-for-priority advertising business, rather than from the actions of third parties."); *Mazur v. eBay Inc.*, No. C 07-03967 MHP, 2008 WL 618988, at *9, 12 (N.D. Cal. Mar. 4, 2008) ("The CDA does not immunize [a content provider] for its own fraudulent misconduct. . . . [Here,] eBay's statement regarding safety affects and creates an expectation

regarding the procedures and manner in which the auction is conducted and consequently goes beyond traditional editorial discretion.”).

15 U.S.C. § 45(a), the FTC contended Accusearch "surreptitiously obtain[ed] and s[old] confidential customer phone records without the customer's knowledge or authorization." Aplt. App., Vol. I at 19 ¶ 1. In reference to Accusearch's business model, the FTC noted that "[f]or a fee, Defendants have offered to obtain 'Details of incoming or outgoing calls from any phone number, prepaid calling card or Internet Phone. Phone searches are available for every country of the world.'" *Id.* at 21 ¶ 9. Further, and most importantly, the FTC alleged (and ultimately proved):

> The account holders have not authorized the Defendants to obtain access to or sell their confidential customer phone records. Instead, to obtain such information, *Defendants have used, or caused others to use, false pretenses, fraudulent statements, fraudulent or stolen documents or other misrepresentations, including posing as a customer of a telecommunications carrier, to induce officers, employees, or agents of telecommunications carriers to disclose confidential customer phone records. Defendants have sold the confidential customer phone records that they have obtained to their clients.*

Id. at 21–22 ¶ 10 (emphasis added).[4] As its cause of action against Accusearch, the FTC claimed "Accusearch violated the FTCA by 'directly or through their employees or agents, . . . obtain[ing] and s[elling] to third parties confidential

[4] To satisfy the injury prong for FTCA liability, the FTC claimed the "invasion of privacy and security resulting from obtaining and selling confidential customer phone records without the consumers' authorization causes substantial harm to consumers and the public, including, but not limited to, endangering the health and safety of consumers." *Id.* at 22 ¶ 11.

customer proprietary network information without the knowledge or consent of the customer.'" *Id.*

[5] If Accusearch had run a traditional business out of a physical location and offered similar services, it would seem the FTC would have the same unfair business practices complaint. Nothing would immunize Accusearch's conduct had it chosen to deliver the confidential telephone records to requesters through hard copy print-outs either in person or through the mail. Accusearch's duty to refrain from engaging in the solicitation and distribution of unlawfully-obtained confidential telephone records should not depend on the medium within which it chooses to operate.

business. In sum, the CDA does not extend to immunize a party's conduct outside the realm of the Internet just because it relates to the publishing of information on the Internet.

Rather than follow the majority's disposition of this issue—extending the definitions of "responsible" and "develop" to include solicitation of information based on consumer selections off of Accusearch's website—I would limit the analysis to whether the CDA even applies in the first place. I would conclude that it does not, and that Accusearch therefore was liable for its unfair business practices in violation of the FTCA.