ORAL ARGUMENT REQUESTED

IN THE UNITED STATES COURT OF APPEALS
FOR THE TENTH CIRCUIT

NO. 08-8003

FEDERAL TRADE COMMISSION,
Plaintiff-Appellee,

v.

ACCUSEARCH, INC., d/b/a ABIKA.COM; and JAY PATEL,
Defendants-Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF WYOMING -- Hon. William F. Downes

BRIEF OF PLAINTIFF-APPELLEE FEDERAL TRADE COMMISSION

WILLIAM BLUMENTHAL
General Counsel

JOHN F. DALY
Deputy General Counsel for Litigation

LAWRENCE DeMILLE-WAGMAN
Attorney
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580
(202) 326-2448

OF COUNSEL:
TRACY S. THORLEIFSON
KIAL S. YOUNG
Federal Trade Commission
Seattle, Washington

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

CASES **PAGE**

STATUTES

MISCELLANEOUS

RELATED APPEALS

There are no prior or related appeals.

JURISDICTION

The Federal Trade Commission ("Commission" or "FTC"), an agency of the United States government, initiated this action in the United States District Court for the District of Wyoming seeking relief for violations of the FTC Act, 15 U.S.C. §§ 41, *et seq.*, committed by defendants Accusearch, Inc. d/b/a Abika.com, and Accusearch's owner, Jay Patel (henceforth, the defendants are referred to as "Accusearch"). The district court's jurisdiction over this matter derives from 28 U.S.C. §§ 1331, 1337(a), and 1345; and from 15 U.S.C. § 53(b).

In its Notice of Appeal, Accusearch seeks review of four orders issued by the district court: 1) the Order and Judgment, which was entered on December 20, 2007 (D.132, Appx. 1605)[1]; 2) the Order on Cross-Motions for Summary Judgment, which was entered on September 28, 2007 (D.120, Appx. 1383); 3) the Order on Plaintiff's Motion to Strike Affirmative Defenses, which was entered on March 28, 2007 (D.118); and 4) the Order Denying Motion to Dismiss, which was entered on July 13, 2006 (D.21, Appx. 101). The Order and Judgment is final and is appealable pursuant to 28 U.S.C. § 1291. Appeal of that order supports appeal of the other three interlocutory orders. *Norton v. The City of Marietta, Oklahoma*, 432 F.3d 1145, 1156 n.8 (10th Cir. 2005).

---

[1] Items in the record are referred to by their district court docket number ("D. xx"). Transcript cites ("Tr.") are referred to by their date. Items that are included in Appellant's Appendix also have an "Appx." cite.

Defendants' Notice of Appeal, which was filed on January 9, 2008, was timely, under Fed. R. App. P. 4(a)(1)(B).

STATEMENT OF THE ISSUES PRESENTED

1) Whether Section 230(c)(1) of the Communications Decency Act, 47 U.S.C. § 230(c)(1), immunizes Accusearch's conduct (*i.e.*, obtaining and selling confidential phone records without consumers' knowledge or consent) from any challenge by the Commission.

2) Whether the Commission lacks authority to bring its law enforcement action against Accusearch, where Accusearch's unfair practices involve the sale of confidential information originally collected by telephone companies subject to the FCC's jurisdiction.

3) Whether the district court abused its discretion or violated the Constitution when, having found that Accusearch engaged in unfair practices, it entered injunctive relief against Accusearch.

STATEMENT OF THE CASE

A. Nature of the Case, the Course of Proceedings, and the Disposition Below

The Commission's complaint alleged that Accusearch engaged in unfair practices by obtaining and selling confidential consumer telephone records without consumers' knowledge or authorization. Accusearch procured these records from

various vendors who could only obtain them by deception or other illegal means. The district court granted the Commission's motion for summary judgment. The court held that Accusearch's practices were unfair, thereby violating the FTC Act, because they caused substantial injury to consumers, the injury was not reasonably avoidable, and the injury was not offset by any benefits. The court rejected Accusearch's contention that, pursuant to the Communications Decency Act, it was exempt from prosecution. The court then imposed injunctive relief, prohibiting Accusearch from selling certain types of personal information, including telephone records, unless it could obtain that information legally. Accusearch has appealed the district court's judgment.

B. Facts and Proceedings Below

1. Background

The Commission commenced the underlying action in May 2006 by filing a complaint in the United States District Court for the District of Wyoming. D.1. The complaint was brought pursuant to Section 13(b) of the FTC Act, 15 U.S.C. § 53(b). It alleged that Accusearch, Inc., and its sole owner and officer, Jay Patel, had violated Section 5(a) of the FTC Act [2] by obtaining and selling consumers' confidential

[2] Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits, *inter alia*, "unfair or deceptive acts or practices in or affecting commerce." Section 13(b), 15 U.S.C. § 53(b), provides that "in proper cases the Commission may seek, and after proper proof, the [district] court may issue, a permanent injunction."

telephone records to third parties without the consumers' knowledge or authorization. The complaint alleged that Accusearch's practices not only violated consumers' privacy, but also jeopardized their health and safety.

Accusearch sells personal information over the internet. D.75, Ex. 21 at ¶ 5. Since at least 2004, and until 2006, Accusearch sold, *inter alia*, confidential consumer telephone records without consumers' permission. In particular, it touted its business by claiming that it could obtain "Details of incoming or outgoing calls from any phone number, prepaid calling card or Internet Phone. Phone searches are guaranteed and available for every country in the world." D.120 at 3 (Appx. 1385). Accusearch advertised that the information it was selling would typically "include the date, time and duration of calls." *Id.* Accusearch's website claimed that its service would be valuable for anyone wanting to check on the background of "Dates, Lovers, [or] Spouses," and for locating "Co-workers * * * [or] ex-spouses." D.78 at Ex. 12 (Appx. 1315, 1318). Call detail records such as those sold by Accusearch can reveal intimate details about a person's lifestyle, business affiliations, or social relationships. D.58 at Ex. 6, p. 4-6, 21-25. They may be used to threaten an individual's reputation, employment status, or physical safety. *See id.*

However, federal law prohibits telephone companies from disclosing the very

sort of telephone records that Accusearch was selling.[3] As a result, the information it sold could be obtained only by theft, by deception (*i.e.*, by impersonating the consumer who was the target of the search), by hacking the telephone company's computer system, or by bribing a telephone company employee to steal the records. D.75, Ex. 41.

Those wishing to purchase telephone records from Accusearch would place orders on Accusearch's website, www.abika.com. D.58, Ex. 2 at ¶ 4 (Appx. 610-611).[4] Accusearch customers would designate the information they wanted, and the cost of the service depended upon the nature of the information requested. *Id.* Accusearch's price for telephone records ranged from $80 to $225. D.58, Ex. 3 at 18. After receiving an order for telephone records from a customer, Accusearch would contact one of its vendors. D.58, Ex. 2 at ¶¶ 3, 5 (Appx. 610, 611). Accusearch's vendors, which consisted of various companies or individuals, would obtain the

[3] Pursuant to 47 U.S.C. § 222, and its implementing regulations, 47 C.F.R. §§ 64.2001-64.2011, telephone companies are prohibited (with certain exceptions not relevant here) from disclosing details of their customers' telephone calls (*i.e.*, date, number called, time, and duration) unless they first obtain their customers' consent. Accusearch sold this sort of information, and there was no consent prior to the disclosure of the information. *See, e.g.*, D.75, Exs. 22-29, 31-33.

[4] Although this case concerns telephone records, Accusearch sold, and, in some instances, has continued to sell, a wide variety of other information, including social security number verification, department of motor vehicle records, GPS traces (pinpointing the exact location of a cell phone at a given time), and reverse e-mail look-ups. D.120 at 2.

requested confidential telephone records, and forward that information to Accusearch. Accusearch would then supply the information to its customers. *Id.* Accusearch's customers communicated only with Accusearch; they did not know who was actually conducting the search. *Id.* If, after the start of a search, a vendor needed additional information to complete the search, the vendor would request that information from Accusearch, and Accusearch would forward the request to its customer. *Id.* at ¶ 7 (Appx. 612-613). Accusearch's customers made payment to Accusearch, and Accusearch made payments to the vendors. *Id.* at ¶ 11 (Appx. 614). Accusearch's customers had no contact with Accusearch's vendors. Indeed, Accusearch did not want its customers to learn the identity of any vendor -- it kept its vendors' names secret to prevent its customers, on future orders, from bypassing Accusearch and obtaining the information directly from the vendors. *Id.* at ¶ 5 (Appx. 611). Similarly, Accusearch did not provide the vendors with information regarding the identity of Accusearch's customers. *Id.* at ¶ 6 (Appx. 611-612).

Accusearch also used its website to amass its stable of vendors. D.58, Ex. 3 at 10-11. Although Accusearch advised its vendors that it would only accept the results of searches that had been conducted in compliance with the law, *id.* at 11, in fact, it winked at its vendors' practices. In particular, if a vendor merely stated that it was complying with the law, Accusearch would accept search results regardless of whether the vendor refused to reveal its sources, D.75, Ex. 40 at 226, or refused to reveal its

search techniques, *id.* at 240 (vendor referred to its search techniques as "trade secrets"). Accusearch accepted information from one vendor that, when questioned regarding the legality of its techniques, merely stated that it obtained the information it was supplying to Accusearch from other companies. *Id.* at 246.

Despite its vendors' assurances, Accusearch had ample evidence that its vendors' searches were not conducted according to law. Accusearch knew that its vendors attempted to break into password-protected accounts. D.75, Ex. 19 at Att. A, p.10. It knew that its vendors used "inside sources" to evade privacy protections. *Id.* at p.6. It knew that its vendors continued to access accounts even as the individuals being spied on attempted to shield their accounts. *Id.* at 28.

Accusearch's invasions of privacy caused substantial harm. Stalkers and other abusers can use telephone records to locate their victims, identify their victims' friends and associates, and monitor their behavior. D.58, Ex. 5 at 16-21. Moreover, even consumers who did not experience physical danger or economic injury experienced real and substantial emotional harm. For example, one female who was targeted by Accusearch was "startled" to discover (as a result of the Commission's investigation), that Accusearch had sold several months' worth of her confidential telephone records to a male former co-worker.

> My husband and I are deeply disturbed and upset to know that this person has spent a good deal of money and effort to obtain our cellular telephone records. We are frightened and anxious, particularly because

> this has been going on so long, suggesting that the person involved has been obsessively interested in us and our records.

D.75, Ex. 25 at ¶ 14. Another target, again a female, was distraught to discover that Accusearch had sold her telephone records to an abusive ex-boyfriend who was stalking her, and who had used those records to locate her. D.75, Ex. 27. A third Accusearch target, a male, was victimized by his ex-wife. She used Accusearch to obtain unlisted cell phone numbers, and then she placed harassing telephone calls to the man and his sons. As a result, the man obtained a domestic violence protective order against his ex-wife. D.75, Ex. 29. Accusearch's practices also imposed monetary costs on consumers. One consumer spent $400 to cancel a cell phone account to which Accusearch had obtained access. D.75, Ex. 25.

2. Proceedings below

The Commission's complaint against Accusearch and Patel contained one count (Appx. 18). It alleged that, by obtaining and selling confidential telephone records without the knowledge or consent of the consumers, defendants had engaged in an unfair practice in violation of Section 5 of the FTC Act, 15 U.S.C. § 45. On June 6, 2006, Accusearch filed a motion to dismiss, pursuant Fed. R. Civ. P. 12(b)(6), arguing, *inter alia*, that the Commission was, without authority, attempting to enforce 47 U.S.C. § 222, the provision of the Telecommunications Act of 1996 that restricts telecommunication carriers from freely distributing the details of their customers'

telephone calls. D.15 (Appx. 25). On July 13, 2006, the court denied Accusearch's motion, holding that the Commission's complaint stated a claim for relief for violations of Section 5 of the FTC Act, 15 U.S.C. § 45. Tr. 7/13/2006, at 23 (Appx. 96).

Both Accusearch and the Commission filed motions for summary judgment. In its two motions, Accusearch argued that its conduct was immune, pursuant to Section 230 of the Communications Decency Act ("CDA"); that, as a matter of law, the Commission could not establish that Accusearch violated the FTC Act; that the Commission was not entitled to injunctive relief; that the Commission was equitably estopped from challenging Accusearch's conduct; and that the Commission lacked jurisdiction to pursue Accusearch. D.45, D.77 (Appx. 106, 1216). In the Commission's motion, it argued that there were no issues of material fact, and that it was entitled to judgment as a matter of law. D.74 (Appx. 903).

On September 28, 2007, the district court granted the Commission's motion, and denied Accusearch's motions. D.120 (Appx. 1383). The court observed that, for Accusearch to prevail on its claim for immunity under the CDA, it would have to show 1) that it was a provider or user of an interactive computer service; 2) that the Commission's claims treated it as the publisher or speaker of the information; and 3) that it did not create or develop, in whole or in part, the information content at issue. With respect to the first part of the test, the court held that, because Accusearch

operated a website, it was a provider or user of an interactive computer service. D.120 at 8 (Appx. 1390). However, the court held that Accusearch could not satisfy the second part of the test: Accusearch was not a "publisher" because it was not merely delivering e-mail containing ill-gotten telephone records. It was critical to the court that it was Accusearch that was soliciting customer orders, that it was Accusearch that was purchasing records from its vendors for a fee, and that it was Accusearch that was reselling those records to its customers. D.120 at 11 (Appx. 1393). Finally, the court held that Accusearch failed the third part of the test as well because, by soliciting the misappropriation of telephone records and purchasing them for resale, it participated in the creation or development of the information. D.120 at 13 (Appx. 1395).

Next, the court held that Accusearch's practices were unfair, and that, as a result, they violated the FTC Act. In particular, the court concluded that Accusearch's conduct met all the elements of unfairness. First, Accusearch caused substantial injury to consumers by providing confidential telephone records to third parties, including stalkers and abusers, without consumers' knowledge or consent. Accusearch also caused economic injury to consumers who, as a result of the breach of the privacy of their telephone records, changed telephone carriers or installed security protections. In addition, the court found that Accusearch's practices caused "substantial and real" emotional injury to consumers whose privacy was invaded. Second, consumers could not reasonably avoid the injury because Accusearch

obtained telephone records without consumers' knowledge or consent. And third, there were no countervailing benefits that resulted from Accusearch's practice of illicitly obtaining and selling confidential telephone records. D.120 at 13-19 (Appx. 1395-1401).

The court rejected Accusearch's defense of equitable estoppel because its contention that others were engaging in the same sort of conduct was not a sufficient basis for this defense. D.120 at 21 (Appx. 1403). It also noted that, in denying Accusearch's motion to dismiss, it had already rejected Accusearch's lack-of-jurisdiction defense. D.120 at 22 (Appx. 1404). Finally, the court held that injunctive relief would be appropriate even though Accusearch was no longer selling telephone records. In particular, the court noted that Accusearch was still selling other forms of personal information (including social security number verification, DMV records, medical records), and that with respect to the sale of that information, it could engage in conduct similar to the illegal conduct it had previously engaged in. D.120 at 20 (Appx. 1402).

On December 20, 2007, the court entered its Order and Judgment for Permanent Injunction and Equitable Relief. D.132 (Appx. 1605). Paragraph I of the Order banned Accusearch from selling telephone records or other consumer personal information derived from telephone records unless it obtained that information in a manner that was clearly permitted by law, regulation, or court order. D.132 at 3

(Appx. 1607). Paragraph II of the Order prohibited Accusearch from: 1) purchasing or selling any consumer personal information unless that information was lawfully obtained from publicly available sources; 2) using false or deceptive representations to obtain consumer personal information; and 3) requesting or purchasing consumer personal information from any person unless it has a reasonable basis to believe that the person obtaining the information will do so lawfully. D.132 at 4 (Appx. 1608). Paragraph III of the Order required Accusearch to assist the Commission in providing a notice to consumers whose records Accusearch sold. That notice will inform those consumers, *inter alia*, of the date their records were sold, and the name of the person to whom they were sold. D.132 at 4 (Appx. 1608). Paragraph IV of the Order required Accusearch to disgorge $199,692.71 to the Commission as equitable monetary relief. D.132 at 6 (Appx. 1610).

Accusearch filed its Notice of Appeal on January 9, 2008. D.133 (Appx. 1619).

STANDARD OF REVIEW

Accusearch argues that, pursuant to § 230(c)(1) of the CDA, its conduct is exempt from the FTC Act. It also argues that it is exempt because the Telecommunications Act does not apply to its conduct. Both of these are issues of law, which this Court reviews *de novo*. *Trujillo v. Cyprus Amax Minerals Co. Ret. Plan. Comm.*, 203 F.3d 733, 736 (10th Cir. 2000). It reviews the district court's grant of injunctive relief for an abuse of discretion. *Australian Gold, Inc. v. Hatfield*, 436

F.3d 1228, 1242 (10th Cir. 2006). That is, this Court should accept the district court's findings of fact unless they are clearly erroneous, and may review the court's application of legal principles *de novo*. *Id.*

SUMMARY OF ARGUMENT

Accusearch does not dispute that it engaged in the conduct challenged by the Commission, or that its conduct caused substantial injury that consumers could not avoid, or that it violated the FTC Act. Instead, it claims that, pursuant to § 230(c)(1) of the CDA, it is altogether exempt from the FTC Act. But, as the district court observed, applying that exemption to Accusearch is like fitting a square peg into a round hole. In particular, Congress enacted that exemption to promote the internet as an interactive public forum. Accusearch does nothing to further that goal because its website is not interactive, *i.e.*, it does not offer any sort of forum for the public. (Part I.A, *infra*.)

Accusearch also fails to satisfy any of the three statutory requirements for § 230(c)(1) immunity. First, it cannot show that it is a "provider or user of an interactive computer service." The district court mistakenly believed that any user of the internet would satisfy this requirement. But to fit within this requirement, an entity must offer an interactive service, such as an internet bulletin board. Section 230(c)(1) shields those who offer such interactive services from liability for statements posted by members of the public. Accusearch cannot be subjected to this

sort of liability because its website is not interactive, and no member of the public can post on it. (Part I.B, *infra*.)

Accusearch cannot meet the second requirement for § 230(c)(1) immunity because the Commission's complaint does not "treat[] [it] as the publisher or speaker" of any information. In fact, the Commission has challenged Accusearch's business of procuring and selling confidential telephone records without consumers' knowledge or consent. Nothing in the complaint challenges publishing or speaking. None of the cases cited by Accusearch advances its cause because in each of those cases, the plaintiff sought to hold the defendant liable solely as a result of the defendant's dissemination of statements made by others, or dissemination of information regarding actions taken by others. Accusearch's liability in this case derives from its own conduct, not because of information disseminated on its website. (Part I.C, *infra*.)

Accusearch cannot satisfy the third requirement for § 230(c)(1) immunity because the Commission is not seeking to hold it liable for "information provided by another information content provider." In fact, the Commission's complaint seeks to hold Accusearch liable for the creation or development of the confidential telephone records that it sold. It solicited orders for the records, and then it instructed its vendors to obtain those records. Thus, Accusearch's liability is based on its own conduct, not the conduct of another. (Part I.D, *infra*.)

Accusearch mistakenly suggests that, because the Telecommunications Act of 1996 prohibits telecommunications carriers from disclosing customer telephone records, including the records that Accusearch was selling, Accusearch's dissemination of those records is somehow exempt from the FTC Act. It is true that the Telecommunications Act does not apply to Accusearch, but nothing in that Act repeals the consumer protections of the FTC Act. The dissemination of confidential telephone records is regulated by more than one statute, and the FTC Act clearly applies to Accusearch. (Part II, *infra*.)

The district court did not abuse its discretion by entering injunctive relief against Accusearch. The evidence shows that its violations are likely to recur, and there is ample opportunity for recurrence because Accusearch is still in the business of selling confidential personal information. And, although Accusearch had ceased its illegal conduct prior to the filing of the Commission's complaint, it did so when its conduct was already under investigation. Such eleventh-hour conversions do not obviate injunctive relief. (Part III.A, *infra*.)

Finally, there is no merit to any of the constitutional arguments that Accusearch raises. The injunctive relief implicates, at most, the First Amendment's intermediate level of scrutiny for restrictions on commercial speech, and it easily satisfies the three-part test for such restrictions. First, the government has a substantial interest -- protecting consumer privacy. Second, the relief furthers that interest by keeping

confidential telephone records out of the hands of stalkers, abusers, and others who have no right to see them. Third, the restrictions are narrowly tailored because they prohibit the very sorts of privacy infringements that the Commission seeks to prevent. Nor are Accusearch's Fifth Amendment due process rights violated by the fact that the injunctive relief applies not just to telephone records but to its sale of any illegally obtained personal information. Because Accusearch has been found guilty of violating the FTC Act, it must expect some fencing-in, preventing it from employing the same illegal practices in other aspects of its business. Finally, although Accusearch alleges unconstitutional selective prosecution, it cannot establish any element of such a violation -- it cannot show bad intent, or that it is a member of a constitutionally protected class, or that others outside that class were not prosecuted. (Part III.B, *infra*.)

ARGUMENT

I. THE DISTRICT COURT CORRECTLY HELD THAT § 230(c)(1) OF THE CDA DOES NOT IMMUNIZE ACCUSEARCH'S ILLEGAL CONDUCT

Accusearch does not dispute that, in connection with its sale of confidential telephone records, it engaged in unfair practices in violation of the FTC Act. That is, it does not challenge the district court's conclusion that its practices (*i.e.*, sale of confidential telephone records to third parties, such as stalkers and abusers, without the consumers' consent) caused substantial injury to consumers, that consumers could

not reasonably avoid this injury, and that Accusearch's practices produced no offsetting benefits. Instead, it argues that, pursuant to § 230(c)(1) of the CDA, its practices are immune from prosecution. However, as the district court correctly held, the immunity provided by § 230(c)(1) simply does not apply to Accusearch's conduct: "in urging this application of the CDA, Defendants ask this Court to fit a square peg into a round hole." D.120 at 6 (Appx. 1388). That is, immunizing Accusearch's conduct would be contrary to congressional intent. Moreover, to qualify for immunity under § 230(c)(1), Accusearch must meet three requirements. But it cannot meet any one of those requirements, let alone all three.

A. The CDA balances the promotion of the internet with the protection of consumer privacy

Section 230 of the CDA was enacted to further two goals. First, it seeks "to promote the continued development of the Internet and other interactive computer services and other interactive media." With respect to this goal, this Court noted that Congress wanted to make sure that the internet could continue to "'offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.'" *Ben Ezra, Weinstein, and Co., Inc. v. America Online, Inc.*, 206 F.3d 980, 985 n.3 (10th Cir. 2000), quoting 47 U.S.C. § 230(a)(3). The section's second goal is to remove "disincentives for the development and utilization of blocking and filtering technologies that empower

parents to restrict their children's access to objectionable or inappropriate online material," while at the same time "ensur[ing] vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer." 47 U.S.C. §§ 230(b)(1), (4), (5).

To promote these two goals, § 230(c) provides two exemptions from liability. The first exemption, set forth in § 230(c)(1), furthers the first goal, *i.e.*, promotion of the internet:

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

§ 230(c)(1). This exemption:

> precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions -- such as deciding whether to publish, withdraw, postpone or alter content -- are barred.

Zeran v. America Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).

The second exemption, set forth in § 230(c)(2), furthers the second goal by immunizing those internet service providers that filter offensive material.[5] Congress

---

[5] Section 230(c)(2) provides:

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

enacted this second exemption to overturn *Stratton-Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. Ct. 1995). *See* H. Conf. Rep. No. 104-458, at 194 (1996), *reprinted at* 1996 U.S.C.C.A.N. 10, 207-208. In *Stratton-Oakmont*, the court held that, because Prodigy had voluntarily deleted some messages on the basis of offensiveness and bad taste, it therefore became legally responsible for messages that it failed to delete.

This case concerns only the first exemption. Although Accusearch claims that § 230(c)(1) exempts it from liability for its violations of the FTC Act, it is mistaken. Plainly, Accusearch does not promote the goal the exemption seeks to further: its website does not provide the public with any sort of forum, and its sale of confidential telephone records does nothing to promote "diversity of political discourse," or "opportunities for cultural development," or "intellectual activity." Because it would be contrary to the purpose of § 230 to apply its immunity to Accusearch, there is little wonder that Accusearch fails to satisfy any of the requirements for immunity under § 230(c)(1).

B. Accusearch cannot satisfy the first requirement for § 230(c)(1) immunity because it is not a provider or user of an interactive computer service

The district court held that Accusearch satisfied the first of the three immunity

---

(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 [subparagraph A].

requirements, simply because it operated a website. *See* D.120 at 8 (Appx. at 1390). But on this point, the district court was mistaken. In particular, Accusearch cannot satisfy this requirement because, during the relevant period, its website did not allow for any interaction between third parties. Thus, it did not offer an *interactive* computer service.

To satisfy the first immunity requirement, an entity must be a "provider or user of an interactive computer service." The CDA defines "interactive computer service":

> The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

47 U.S.C. § 230(f)(2).[6]

Those for whom this protection is relevant are those who operate internet "bulletin boards," *i.e.*, forums on which members of the public may post information. As *Stratton-Oakmont* shows, internet service providers frequently create such bulletin boards. In that case, Prodigy, the creator of the bulletin board, was an internet service

---

[6] "Access software provider" is defined as:

> a provider of software (including client or server software), or enabling tools that do any one or more of the following:
>
> (A) filter, screen, allow, or disallow content;
>
> (B) pick, choose, analyze, or digest content; or
>
> (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

§ 230(f)(4).

provider. In other situations, the bulletin boards may be created not by an internet service provider, but by a user that is not itself an internet service provider. The user takes advantage of the internet to gain access to a wide audience. Amazon.com is a user that creates bulletin boards on which members of the public may post comments regarding the books Amazon offers for sale. *See Universal Communication Systems, Inc. v. Lycos, Inc.*, 478 F.3d 413, 415 (1st Cir. 2007) (a "user" of Lycos' service created a bulletin board on which the public could post comments regarding a publicly held company). Regardless of whether the bulletin board is created by the provider of the interactive computer service, or a user of that service, § 230(c)(1) seeks to shield that creator from liability for statements posted by members of the public.

By no stretch of the imagination is Accusearch a provider of an interactive computer service. It operated as a store front through which its customers engaged in private commercial transactions. The only interaction was between Accusearch and its customers, or between Accusearch and its vendors. Thus, it simply did not provide a "service, system, or access software" that "enables computer access by multiple users." Indeed, there is no indication in the record that Accusearch "enable[s] computer access" to anyone at all. Nor is Accusearch a "user" in the limited sense of § 230(c)(1).

Accusearch repeatedly claims that it "operates" an "interactive" search service.

See Br. at 10, 13, 33, 34, 35.[7] In fact, however, the uncontested declaration of Accusearch's former employee, Rhiannon Martinez, explains that, during the period challenged by the Commission, Accusearch's customers had no contact whatsoever with Accusearch's vendors. Indeed, Accusearch took steps to make sure that its customers never even learned the identity of the vendors who conducted the searches that generated the information the customers purchased. D.58, Ex. 2 at ¶ 5-6 (Appx. 611-612). The only evidence that Accusearch cites consists of two declarations from defendant Patel. Both were dated well after the events that are the subject of the Commission's complaint, and both are cleverly written in the present tense. *See* Appx. 144, 1245. At the time those declarations were written (December 2006, January 2007), Accusearch had modified its business model and was no longer operating as it had during the period challenged in the Commission's complaint (March 2003 until January 2006). *See* D.58 at 4 (Appx. 395). Thus, during the relevant time period, there was nothing whatsoever that was "interactive" about Accusearch's website: it bore no resemblance to an internet bulletin board. Accordingly, Accusearch was not a provider or user of an interactive computer service and could not satisfy the first part of the test set forth in § 230(c)(1).

Both the district court and Accusearch mistakenly rely on *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003), to support their conclusion that Accusearch was a provider

[7] Cites to Accusearch's opening brief are referred to as "Br. at xx."

or user of an interactive computer service merely because Accusearch operated a website. *See* D.120 at 8, Br. at 34-35. However, facts of *Batzel* are very different from this case. In *Batzel*, defendant Smith made defamatory statements in an e-mail suggesting that Batzel possessed artworks stolen by the Nazis. He sent this e-mail to defendant Cremers, who posted it on a museum security website that Cremers controlled, and sent it to subscribers of a museum security internet newsletter that Cremers assembled. The Ninth Circuit panel held that, because Cremers used the internet to post the website and distribute the newsletter, he was a "user" of an interactive computer service, and thus satisfied the first part of the § 230(c)(1) test. The facts of *Batzel* bear little resemblance to Accusearch's illegal conduct. The plaintiff in *Batzel* sought to hold defendant Cremers liable for statements of a third party (defendant Smith) merely because Cremers posted them on the internet. Here, the Commission seeks to hold Accusearch for its own conduct -- procuring and selling confidential telephone records.

Moreover, the Ninth Circuit, sitting *en banc*, recently stated that it had doubts as to the correctness of the *Batzel* panel's determination that the defendant was a user of an interactive computer service. *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1170 n.28 (9th Cir. 2008) (*en banc*). The problem with *Batzel* is that, with respect to the first immunity requirement (the entity must be a "provider or user of an interactive computer service"), the panel's

interpretation ignores the word "interactive." But no statute should be interpreted in a manner that renders any term superfluous. *Andersen v. Director, Office of Workers' Compensation Programs*, 455 F.3d 1102, 1106 (10th Cir. 2006). Moreover, the panel's broad interpretation in no way furthers Congress's purpose, which was to preserve the unique interactive aspect of the internet, *see* § 230(b)(2), because it was far from clear that there was anything interactive about Cremers's website or newsletter.[8]

The other cases cited by the district court, and by Accusearch, also involve situations that are very different from this case. For example, in *Schneider v. Amazon.com, Inc.*, 31 P. 3d 37 (Wash. Ct. App. 2001), Schneider sued Amazon regarding defamatory comments that had been posted on that portion of Amazon's website that permits members of the public to make comments regarding books that Amazon sells. The court, citing *Zeran*, noted that the purpose of § 230(c)(1) immunity

[8] The district court and Accusearch also cite *Almeida v. Amazon.com, Inc.*, 2004 WL 4910036 (S.D. Fla. 2004), *aff'd on other grounds*, 456 F.3d 1316 (11th Cir. 2006). D.120 at 8, Br. at 34. That court held, without any elaboration, that it was "irrefutable" that Amazon was an interactive computer service because "[i]ts primary function is to allow multiple users to a computer service the ability to purchase various items, including but not limited to, books." *Id.* at *4. Again, this holding (which the Eleventh Circuit, on review, stated was unnecessary to the resolution of the case, 456 F.3d at 1324) is too broad because it would give any website operator a free pass through the first part of the § 230(c)(1) immunity test. Although some aspects of Amazon's website are, indeed, interactive, *see infra*, those aspects that were at issue in *Almeida* were not. There is nothing interactive if a website operator merely allows members of the public to purchase items that the operator is selling.

is to shield companies that "serve as intermediaries for other parties' potentially injurious messages." *Id.* at 41, citing *Zeran*, 129 F.3d at 330-31. The court correctly recognized that, with respect to this aspect of its operation, Amazon was a provider or user of an interactive computer service, not just because it operated a website, but because its website included the interactive forum on which anyone could post comments.[9]

Accusearch is a "provider or user of an interactive computer service" only if that phrase is interpreted so broadly that the word "interactive" becomes superfluous.

---

[9] The other cases cited by Accusearch are similar to *Schneider*, *see* Br. at 23, because they involve entities that provided interactive use of the internet. In *Gentry v. eBay, Inc.*, 99 Cal. App. 4th 816 (2002), the plaintiffs sued eBay as a result of counterfeit sports memorabilia that had been sold through eBay's website. The court held that, because eBay was not the seller, but merely provided an internet forum on which third parties could make sales, eBay was a provider or user of an interactive computer service. *Id.* at 831 n.7. In *Carafano v. Metrosplash.com, Inc.*, 207 F. Supp. 2d 1055 (C.D. 2002), *aff'd*, 339 F.3d 1119 (9th Cir. 2003), the plaintiff, a TV star, brought an action for defamation and other torts against an internet dating service as a result of a fake and defamatory dating profile that had been posted by an anonymous member of the public. The court held that, because members of the public are able to "access and use," *i.e.*, add to, Metrosplash's data base, Metrosplash is a provider or user of an interactive computer service with respect the information posted by the public. *Id.* at 1065-66. In *Parker v. Google*, 422 F. Supp. 2d 492 (E.D. Pa. 2006), plaintiff alleged that a search of his name through Google's search function would lead to defamatory websites. Pursuant to § 230(f)(4)(C), Google, which organizes, caches, and permits the search of internet information, is clearly an access software provider, and, pursuant to § 230(f)(2), is therefore a provider of an interactive computer service. Finally, in *Donato v. Moldow*, 865 A.2d 711 (N.J. Super. Ct. App. Div. 2005), the defendant was sued regarding defamatory comments that were posted on an internet bulletin board that he operated. Clearly, the defendant was a provider or user of an interactive computer service. Accusearch's business bears no similarity to any of these cases.

Such an interpretation stretches the exemption provided by § 230(c)(1) far beyond the purposes set forth by Congress. Because Accusearch's website only offered customers the ability to purchase a product, not any opportunity for interaction, this Court should hold that Accusearch cannot satisfy the first requirement for immunity under § 230(c)(1).

C. The district court correctly held that Accusearch cannot satisfy the second requirement for § 230(c)(1) immunity because the Commission's complaint does not treat it as a publisher or speaker

As the district court correctly recognized, the Commission's complaint challenges Accusearch's practice of obtaining and selling confidential telephone records, not its publication (or speaking) of any information. D.120 at 9-12 (Appx. 1391-94). The court noted that Accusearch might have been able to satisfy this second requirement if it "merely delivered an email containing ill-gotten consumer phone records. Clearly, that is not the type of conduct at issue here." D.120 at 11 (Appx. 1393). What the Commission has challenged is the practice of selling illegally obtained telephone records, a practice that causes substantial consumer injury, and that violates the FTC Act. In particular, as explained by Rhiannon Martinez, Accusearch's former employee, D.58, Ex. 2 (Appx. 610), and as found by the district court, D.120 at 3 (Appx. 1385), Accusearch sold telephone records that it could obtain only through improper means.

That Accusearch was acting as a seller of information, not as a publisher of

information sold by others, is clear from the manner in which it conducted its business. Each time it received an order for such records, it selected one of its vendors and transmitted that order to the vendor. When it transmitted the order, it made sure that the vendor could not identify the customer who had placed the order. After the vendor had obtained the records (through computer hacking, deception, illegal insider contacts, etc.), the vendor provided that information to Accusearch. Before Accusearch conveyed the information to its customer, it made sure that the customer could not identify the vendor who had supplied the information to Accusearch. The customer paid Accusearch for the search results, based on prices set forth on Accusearch's website. Accusearch paid its vendors for the information they supplied based upon its agreements with the vendors.

The Commission alleged that Accusearch's "practices in obtaining and selling to third parties confidential customer phone records" without the consumer's knowledge or consent constituted an unfair practice that violated the FTC Act. D.1 (Appx. 18). Nothing in the complaint challenges publishing or speaking. Indeed, as the district court recognized, treating Accusearch as a publisher would be inconsistent with the purpose of the immunity set forth in § 230(c)(1). *See* D.120 at 11 (Appx. 1393).

None of the cases cited by Accusearch, Br. at 27-28, advances its cause because they involve entities whose business model was very different from Accusearch. *See*

D.120 at 11 (Appx. 1393) (district court recognized that Accusearch was not a "publisher" because it was not merely delivering e-mails). In each of those cases, the defendant provided a means through which others were able to publicize information through the internet, and the issue was whether the entity providing such means could be held liable for the underlying communication. For example, in *Ben Ezra*, *see* Br. at 27, the plaintiff sued America Online for negligence and defamation, based on allegedly inaccurate stock price information that third parties had posted on America Online's Quotes & Portfolio service area. 206 F.3d at 983. Because America Online's only role was the transmission of the price information, the court held that it was entitled to immunity.[10] By contrast, Accusearch had a much broader role.

In another case cited by Accusearch, *Stoner v. eBay, Inc.*, 2000 WL 1705637 (Cal. Super. 2000), *see* Br. at 29, a provider or user of an interactive computer service (eBay) was sued solely for its role in conveying information regarding an illegal product (sound recordings that violated copyright laws) to the public. A third party was the marketer of the recordings, and there was no allegation that eBay had any role in their production. As the court explained, "[a] principal objective of the

[10] Similarly, in *Zeran*, *see* Br. at 27, the court held that America Online was entitled to immunity because the plaintiff sought to hold it liable for defamatory statements made by another, and America Online's only role was that it provided the means through which that other party could publicize those statements. 129 F.3d at 330. The defendants in *Metrosplash*, *see* Br. at 27, and in *Schneider v. Amazon*, *see* Br. at 32, were entitled to immunity for the same reason. 339 F.3d at 1122; 31 P. 3d at 38-39.

[§ 230(c)(1)] immunity provision is to encourage commerce over the Internet by ensuring that interactive computer service providers are not held responsible for how third parties use their services." *Id.* at *3. That is, just as an interactive computer service is not liable for information it merely publishes, the court in *Stoner* held that eBay, which provides an interactive marketing service, is not liable for a product sold by a third party where the service's only role is conveying information regarding the availability of that product to the public.[11] Accusearch's role was completely different.

The Commission's case against Accusearch challenges Accusearch's procuring and sale of confidential consumer telephone records without the knowledge of the

---

[11] *See also Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666 (7th Cir. 2008) (Br. at 31) (court held that craigslist, an online meeting place, was not liable for ads that violated the Fair Housing Act and that were placed on its site by third parties); *Beyond Systems, Inc. v. Keynetics, Inc.*, 422 F. Supp 2d 523 (D. Md. 2006) (Br. at 27) (court held that defendant Rackspace, Ltd., an internet service provider, was immune where the only source of its liability was the transmission of illegal e-mails that originated with a third party); *Barnes v. Yahoo!, Inc.*, 2005 WL 3005602 (D. Or. 2005) (Br. at 28) (court held Yahoo was immune where its liability was based solely on a false internet profile that plaintiff's ex-boyfriend had posted); *Doe v. Bates*, 2006 WL 3813758 (E.D. Tex. 2006) (Br. at 28) (Yahoo was immune from liability for child pornography that appeared on an interactive web-based forum hosted on its website); *Doe v. America Online, Inc.*, 783 So. 2d 1010 (Fla. 2001) (Br. at 28) (America Online was not liable for child pornography marketed by a third party through an America Online chat room); *Doe v. MySpace, Inc.*, 474 F. Supp. 2d 843 (W.D. Tex. 2007), *aff'd*, 2008 WL 2068064 (5th Cir. 2008) (Br. at 28) (MySpace, which allows members of the public to post online profiles, was immune from the consequences of information on such a profile that was created by a third party).

consumer. This is not a case in which liability is based on publication or speaking. Accordingly, Accusearch cannot satisfy the second requirement for § 230(c)(1) immunity.

D. The district court correctly held that Accusearch cannot satisfy the third requirement for § 230(c)(1) immunity because the information on which Accusearch's liability was based was not provided by another information content provider

As the district court correctly concluded, Accusearch could not satisfy the final requirement for § 230(c)(1) immunity because the Commission challenged it for *its* role as an information content provider. In particular, the court found it significant that it was as a result of Accusearch's efforts that the telephone records were misappropriated and transmitted to its customers. D.120 at 13 (Appx. 1395).

The CDA defines "information content provider":

> The term "information content provider" means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

§ 230(f)(3). In fact, Accusearch was most definitely "responsible, in whole or in part, for the creation or development" of the information that it sold to its customers. It advertised that it could obtain confidential telephone records, and, when it received an order for such records, it fulfilled that order by contacting one of its vendors, and instructing that vendor to obtain the records.

Accusearch contends that it was not an information content provider because

it did not create the confidential telephone records -- it notes that the district court observed that those records were originally created by telephone companies. Br. at 36-37. But Accusearch ignores the next sentence in the court's order: "As a result of [Accusearch's] business efforts, [the records] were subsequently misappropriated and ultimately transmitted via [Accusearch's] website to end-consumers." D.120 at 13 (Appx. 1395). That is, the information that is at issue here is illegally obtained telephone records of particular consumers, not simply the underlying data base of all calls maintained by the telephone company. And although it was Accusearch's vendors that wrongfully obtained the records, Accusearch was "responsible" for that conduct because the vendors obtained those particular records only after receiving a specific request for those records from Accusearch.[12]

Accusearch mistakenly contends that its conduct is akin to that of the defendant in *Chicago Lawyers' Committee v. Craigslist, supra*. In particular, it twists its own situation and argues that it "cannot be found to have created or to have 'participated in the creation' of telephone records simply by having a forum in which people

[12] Accusearch contends that its solicitation of the telephone records from its vendors should not deprive it of immunity because solicitation is not mentioned in § 230(c)(1). Br. at 39. But, pursuant to § 230(f)(3), an "information content provider" is not just one who creates or develops information, but also includes one who is *responsible* for the creation or development of information. Accusearch is responsible for the telephone records because it orders them from its vendors, *i.e.*, it solicits them. Because it solicits the records, it is an information content provider and it cannot satisfy the third immunity requirement.

advertise and request this information." Br. at 37-38. As the Seventh Circuit explained, defendant craigslist "provides an electronic meeting place for those who want to buy, sell, or rent housing (and many other goods and services)." 519 F.3d at 668. A buyer who sees an item on craigslist knows that the item is being sold by an independent seller, not by craigslist. If the buyer has questions, the buyer contacts the seller directly, not craigslist. And if the buyer chooses to make a purchase, the buyer makes payment to the seller, not to craigslist. The item is then delivered by the seller directly to the buyer, not via craigslist.

Accusearch is very different from craigslist. Accusearch did not provide a "forum," or an "electronic meeting place" because its customers, who wanted to buy information, had no contact whatsoever with Accusearch's vendors. Indeed, Accusearch attempted to make sure that its customers did not know the identity of its vendors, and those customers may not even know that vendors are involved in the process of obtaining the information they have purchased. Thus, Accusearch did not offer any sort of "forum" or "electronic meeting place."

Because of its extensive role in developing the records that it sold, Accusearch is not helped by *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.D.C. 1998); *see* Br. at 29. In that case, plaintiff sued gossip columnist Drudge for defamatory comments that appeared in his Drudge Report. Drudge posted the Report on his website, mailed it to certain e-mail subscribers, and, pursuant to an agreement with America Online,

made it available to all America Online subscribers. That agreement, which had been in effect for several months at the time of the alleged defamation, provided that America Online would pay Drudge $3000 per month in return for the right to include the Drudge Report on its website. Although Accusearch contends that the court found that America Online was responsible for "soliciting" the defamatory statements, *see* Br. at 38, the court found nothing of the sort. The court never held that America Online had "solicited" the defamatory column. In fact, the court concluded that "there simply is no evidence that [America Online] had any role in creating or developing any of the information in the Drudge Report." *Id.* at 50. Even though America Online paid Drudge, the court held that America Online "was nothing more than a provider of an interactive computer service on which the Drudge Report was carried * * *." *Id*. The crucial fact is that America Online did not hire Drudge to write the allegedly defamatory column. Accusearch operated differently because it did solicit the unlawful searches necessary to obtain the telephone records that it sold.[13] Thus, its situation is very different from that of *Blumenthal v. Drudge*.

Accusearch's conduct is more similar to that of the defendant in *Fair Housing Council v. Roommates.com, supra*. In that case, the defendant operated a website designed to match people renting out spare rooms with people looking for a place to

[13] *Ben Ezra v. America Online, supra*, and *Batzel v. Smith, supra, see* Br. at 38, are similar to *Blumenthal v. Drudge*. In neither of those cases did the defendant engage in the sort of solicitation of the information content that Accusearch used.

live. Users of the website had to create a personal profile, and to do so, they were required to specify preference in roommates with respect to various criteria, including sex, sexual orientation, and whether potential renters could or would bring children into the household. 521 F.3d at 1161. Defendant then sent periodic e-mail updates to those who had created profiles, informing them of housing or renters that matched their preferences. Plaintiff alleged defendant violated federal and state fair housing laws by requiring those who used its service to specify preferences with respect to these three criteria. Defendant sought immunity pursuant to § 230(c)(1), but the Ninth Circuit, sitting *en banc*, held that it was an information content provider, and thus not entitled to immunity. "By requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, [defendant] becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information." *Id.* at 1166. The court further explained that defendant was not entitled to immunity because it was responsible "for the predictable consequences of creating a website designed to solicit and enforce housing preferences that are alleged to be illegal." *Id.* at 1170. The court stressed that defendant "both elicits the allegedly illegal content and makes aggressive use of it in conducting its business." *Id.* at 1172.[14]

[14] Accusearch cites *Carafano v. Metrosplash*, *supra*, and claims that the phrase "information content provider" should be narrowly interpreted. Br. at 25-26. In particular, Accusearch cites that portion of *Metrosplash* in which the panel stated that

Accusearch's involvement is at least as extensive as that of the defendant in *Roommates.com*. Like the defendant in that case, Accusearch is responsible "for the predictable consequences" of a business model that both "elicits" illegal conduct and "makes aggressive use of it in conducting its business." Accusearch is therefore much more than a "passive transmitter of information provided by others." It is, at least in part, responsible for the development of that information. That is, it procured the information without the knowledge of the consumer being spied on, and it sold the information without the consumer's consent. Thus, it cannot satisfy the final requirement for § 230(c)(1) immunity.

* * * * *

Accusearch mistakenly contends that the district court denied its request for immunity because of its "discomfort" with respect to the information it was selling, Br. at 42, and that "society as a whole" would benefit if § 230(c)(1) were interpreted

---

a website operator could not be held liable for content submitted by a third party. 339 F.3d at 1124. However, in *Fair Housing Council v. Roommates.com*, the Ninth Circuit, sitting *en banc*, explained that *Metrosplash* should not be read so broadly. "Providing immunity every time a website uses data initially obtained from third parties would eviscerate the exception to section 230 for 'develop[ing]' unlawful content 'in whole or in part.'" 521 F.3d at 1171. Instead, the court explained that Metrosplash was immune because the libelous content was "developed entirely by the malevolent user, without prompting or help from the website operator." *Id.* The key was that in *Metrosplash*, "the website did absolutely nothing to encourage the posting of defamatory content * * *." *Id.* Unlike the website provided by the defendant in *Metrosplash*, Accusearch *did* prompt and encourage its vendors to obtain information that could only be obtained unlawfully.

to immunize its conduct, Br. at 44. In fact, of course, the district court denied immunity not for any policy reasons, but because Accusearch could not satisfy the requirements of § 230(c)(1). Moreover, although § 230(c)(1) immunity is broad, it is not unlimited.

> When Congress passed section 230 it didn't intend to prevent the enforcement of all laws online; rather, it sought to encourage interactive computer services that provide users *neutral* tools to post content online to police that content without fear that through their "good samaritan . . . screening of offensive material," 47 U.S.C. § 230(c), they would become liable for every single message posted by third parties on their websites.

Fair Housing Council v. Roommates.com, 521 F.3d at 1175 (emphasis in original). Because Accusearch is not merely providing "neutral tools" to third parties, the district court in no way trenches on Congress's policy.

II. THE DISTRICT COURT CORRECTLY HELD THAT 47 U.S.C. § 222 DOES NOT OF THE DEPRIVE THE FEDERAL TRADE COMMISSION OF JURISDICTION OVER ACCUSEARCH'S CONDUCT

There is no merit to any of the jurisdictional arguments that Accusearch makes based on the privacy protection provisions of the Telecommunications Act of 1996. It contends that, because those provisions, which prohibit telecommunications carriers from disclosing customer telephone records without consent, apply only to telecommunications carriers, and because Accusearch is not a telecommunications carrier, its dissemination of those records is somehow exempt from challenge under any other law. It also argues that, because the FCC enforces the privacy provisions

of the Telecommunications Act, the Commission is precluded from taking any action that affects the dissemination of such records. Not surprisingly, Accusearch has no authority to support its arguments.

The Telecommunications Act of 1996 protects the privacy of the customer telephone records that Accusearch sold. The Act defines "customer proprietary network information" to mean:

> (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier[.]

47 U.S.C. § 222(h)(1). Customer proprietary network information encompasses the customer telephone records that Accusearch sold. The Telecommunications Act further provides that:

> [e]xcept 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.

47 U.S.C. § 222(c)(1). The Act applies to telecommunications carriers, § 222(a)(1), and it is enforced by the FCC, *e.g.*, 47 U.S.C. § 503(b)(1)(B).

Accusearch makes the absurd suggestion that, because the Telecommunications Act restricts telecommunications carriers from disseminating customer telephone records, any other dissemination of such records must be free from regulation. Br. at 59-60. That is, Accusearch contends that once it obtained protected telephone records (by deception, hacking, etc.) it was free to make any use of those records. This argument ignores that "this is an era of overlapping agency jurisdiction under different statutory mandates." *FTC v. Texaco, Inc.*, 555 F.2d 862, 881 (D.C. Cir. 1977); *Mainstream Marketing Services, Inc. v. FTC*, 283 F. Supp. 2d 1151, 1168 (D. Colo. 2003), *rev'd on other grounds*, 358 F.3d 1228 (10th Cir. 2004). In this case, the FCC regulates the dissemination of customer telephone records by telecommunications carriers, and the Commission has the authority to regulate the practices of others with respect to those records. Nothing in the Telecommunications Act restricts the Commission's jurisdiction over unfair acts or practices, and repeals by implication are disfavored. *Radzanower v. Touche Ross & Co.*, 426 U.S. 148, 154 (1976). Thus, nothing precluded the district court from holding that, even though Accusearch was not subject to the Telecommunications Act, its conduct, which caused substantial consumer injury, was unfair, and, therefore, in violation of the FTC Act.[15]

---

[15] Accusearch contends that, during the period covered by the Commission's complaint, "it was simply not illegal to obtain phone records, *even* through fraudulent means." Br. at 60. Of course, as this case shows, Accusearch is wrong because its conduct was, at all times, subject to the FTC Act's prohibition against unfair or deceptive practices. Moreover, Accusearch is also incorrect, even if it is referring to

Nor is there any merit to Accusearch's suggestion that the Commission was somehow attempting to enforce the Telecommunications Act. *See* Br. at 62-63. As the complaint clearly shows, the Commission alleged that Accusearch violated the FTC Act, not the Telecommunications Act. D.1. However, the Telecommunications Act was certainly not irrelevant to the Commission's case. As explained above, to show that a practice is "unfair" pursuant to the FTC Act, the Commission must show that the practice caused substantial consumer injury. Here, Accusearch caused substantial consumer injury because it obtained confidential consumer telephone records without consumers' knowledge, and made them available, for a price, to third parties including stalkers and abusers. The Telecommunications Act recognizes the potential injury that could result from free access to such telephone records and it attempts to restrict their release. It also recognizes the importance of protecting consumer privacy. The very harm that the Telecommunications Act attempts to prevent is the harm that Accusearch caused by evading the protections of that act.[16]

---

criminal liability. It is true that it was not until 2007 that Congress passed the Telephone Records and Privacy Act, which makes it a crime to sell, transfer, or receive confidential telephone records information. 18 U.S.C. § 1039. However, Accusearch cannot plausibly suggest that, even prior to the passage of that act, it would have been exempt from prosecution if it, or its vendors at its urging, had committed a crime (*e.g.*, theft) to obtain the records.

[16] Accusearch cites four criminal cases, which it contends establish that consumers have no expectation of privacy in their telephone records. Br. at 60. In fact, those cases show nothing of the sort. *Smith v. Maryland*, 442 U.S. 735 (1979), substantially predates the privacy protections of the Telecommunications Act. *United*

Thus, the Telecommunications Act neither precludes the Commission from policing Accusearch's unfair practices nor shields those illegal practices.

III. THE DISTRICT COURT DID NOT ABUSE ITS DISCRETION IN ENTERING INJUNCTIVE RELIEF AGAINST ACCUSEARCH

The district court did not abuse its discretion when, after determining that Accusearch caused substantial consumer injury and violated the FTC Act, it entered an injunction to prevent future violations. That relief was justified by law, and appropriate under the circumstances of this case. Also, the relief did not contravene any provision of the Constitution.

A. The court did not abuse its discretion

It is well established that § 13(b) of the FTC Act, 15 U.S.C. § 53(b), gives the district court "authority to grant a permanent injunction against violations of *any provisions of law enforced by the Commission . . ..*" *FTC v. Evans Products Co.*, 775 F.2d 1084, 1086 (9th Cir. 1985) (emphasis in original), and Accusearch has not

---

States v. Miller, 425 U.S. 435 (1976), is irrelevant because it not only predates the Telecommunications Act, but also concerns the privacy of bank records, not telephone records. And, although *New Hampshire v. Gubitosi*, 886 A.2d 1029 (N.H. 2005), and *Oregon v. Johnson*, 131 P. 3d 173 (Or. 2006), both postdate the Telecommunications Act and involve telephone records, the Act did not protect the records in either case because law enforcement authorities had subpoenaed the records at issue. Pursuant to 47 U.S.C. § 222(c)(1), the privacy protections of the Act do not apply where their release is required by law. *See ICG Communications, Inc. v. Allegiance Telecom*, 211 F.R.D. 610, 612-614 (N.D. Cal. 2002) (where records are sought pursuant to discovery governed by the Federal Rules of Civil Procedure, release is required by law and the protections of the Telecommunications Act do not apply).

argued otherwise. Moreover, when a court has determined that a defendant has violated a law that furthers the public interest, as has happened here, "[t]he critical question for a district court in deciding whether to issue a permanent injunction in view of past violations is whether there is a reasonable likelihood that the wrong will be repeated." *SEC v. Manor Nursing Centers, Inc.*, 458 F.2d 1082, 1100 (2d Cir. 1972).[17]

There is ample evidence in the record that it is reasonably likely that Accusearch's violations will recur. Illegal past conduct creates an inference that future violations will occur. *SEC v. Manor Nursing Centers, id.* This is particularly so given the egregious nature of Accusearch's privacy violation, the harm it caused, *see supra*, and the fact that it knew, or should have known of that harm.[18] In addition,

---

[17] Accusearch cites *Loewen Group Acquisition Corp. v. Matthews*, 12 P.3d 977 (Okla. Civ. App. 2000), and contends that injunctions should be entered "sparingly and cautiously." Br. at 47. But that case is irrelevant because it involved a private lawsuit, not the enforcement of a federal law. Accusearch also cites Chief Justice Burger's separate concurrence in *Aaron v. SEC*, 446 U.S. 680, 703 (1980), in which he refers to injunctive relief as a "drastic remedy." Br. at 47. But Accusearch ignores that Chief Justice Burger also cited with approval *Manor Nursing Centers* and the standard for injunctive relief set forth in that case. In any event, injunctive relief is routinely awarded in cases brought by the Commission to enforce the FTC Act. *See* cases listed at http://www.ftc.gov/os/caselist/index.shtm.

[18] Accusearch claims that it advised its vendors to conduct searches in compliance with the law. Brief of Appellants ("Br.") at 33. But, as explained above, this was mere window dressing because some vendors refused to reveal their search techniques to Accusearch, and Accusearch was aware that others were using deception to obtain the information that Accusearch had solicited. *See* D.75, Ex. 19 at Att. A, pp. 6, 10, 28.

although Accusearch has ceased selling confidential consumer telephone records, the district court found that it is still in the business of selling other personal and private information obtained by its vendors (social security number verification, motor vehicle records, cell phone traces), D.120 at 2 (Appx. 1384), and it could easily resume its past illegal conduct. Finally, Accusearch's attitude is relevant. In particular, defendant Patel, who controls Accusearch, has expressed disdain for individual privacy. *See* D.75, Ex. 45 at Att. A ("I don't even believe in privacy too much"). That is, he puts little stake in the values that underlie both § 222 of the Telecommunications Act and the Commission's case. Clearly, this lack of appreciation for privacy makes it more likely that, in the future, he will violate the law or turn a blind eye to such practices.

None of Accusearch's arguments satisfies its burden of showing that the district court abused its discretion when it entered injunctive relief. *See United States v. W.T. Grant Co.*, 345 U.S. 629, 633 (1953) (defendant bears the "heavy" burden of showing that there is no reasonable expectation that its past violations will be repeated). Accusearch cites to the Telephone Records and Privacy Act, 18 U.S.C. § 1039 ("TRPA"), and claims that no injunction is necessary because its past conduct now violates that law. Br. at 48-49. But a law violation is a predicate to injunctive relief, not a shield against such relief. That is, in a case such as this one, the court must first determine that the law has been violated before it even considers the appropriateness

of injunctive relief. The mere fact that Accusearch's past conduct might now violate two laws (*i.e.*, the TRPA and the FTC Act) instead of just one, is not relevant to the crucial issue -- whether that conduct is likely to recur.

In any event, the TRPA is a criminal law. Not only does the Commission have no authority to enforce that law, but also its prohibitions are not congruent with the FTC Act. Criminal intent is an element of a TRPA violation, but the Commission need not establish intent to show that the FTC Act has been violated. *See FTC v. Freecom Communications, Inc.*, 401 F.3d 1192, 1204 n.7 (10th Cir. 2005) (scienter is not an element of an FTC Act violation). Thus, Accusearch could violate the FTC Act without violating the TRPA.

Nor is the injunctive relief obviated by the fact that, three months before the Commission filed its complaint, Accusearch stopped selling telephone records. *See* Br. at 49-50. Cessation of illegal activities does not deprive the court of its authority to enter injunctive relief. *United States v. W.T. Grant*, 629 U.S. at 633.[19] Nor does cessation, even voluntary cessation, demonstrate that illegal conduct will not recur. This is particularly so where, as here, Accusearch ceased selling telephone records

[19] Accusearch cites *Friends of the Earth, Inc. v. Laidlaw Environmental Services, Inc.*, 528 U.S. 167, 193 (2000), where the Supreme Court noted that cessation of conduct is "an important factor" bearing on the appropriateness of injunctive relief. Br. at 50. But the Court makes clear that cessation is only a factor to be considered; it is not determinative. In a case such as this one, where there are other factors that indicate that Accusearch's illegal conduct is likely to recur, cessation does not undermine the need for injunctive relief.

when its conduct was already under investigation.[20] Also, although Accusearch stopped selling telephone records, it continues to sell other private and personal information.[21] Given the other evidence showing that Accusearch's violations were likely to recur, the mere fact that it ceased selling telephone records shortly before the Commission filed its complaint does not show that the court abused its discretion when it entered injunctive relief.[22]

---

[20] Defendant Patel claims that Accusearch stopped selling telephone records on January 20, 2006. He further claims that Accusearch did so as a result of the fact that it learned that one of its vendors was pretexting (*i.e.*, using deception) to obtain the records. Br. at 14; App. at 1248. But Accusearch had ample evidence well before that time that its vendors were using illegal techniques to obtain records. *See* D.75, Ex. 19 at Att. A, pp. 6, 10, 28. Moreover, in January 2006, Accusearch learned that it was under investigation by the FCC. D.58, Ex. 3 at 20. Courts are well aware that, faced with the prospect of an enforcement action, targets of investigations are all too likely to undergo eleventh-hour conversions and bring their conduct (temporarily) into compliance with the law. *See SEC v. Manor Nursing*, 458 F.2d at 1100 (inference that illegal conduct will be repeated is "particularly appropriate here where appellants did not attempt to cease or undo the effects of their unlawful activity until the institution of an investigation").

[21] Accusearch notes that, in February 2006, the Commission's staff sent letters to other entities that were selling consumer telephone records, warning that those entities might be violating the law. Accusearch inferred that it did not receive such a letter because it had already ceased selling telephone records. In fact, at the time the Commission's staff sent out the warning letters, the Commission's investigation of Accusearch was already well under way. As a matter of course, the Commission's staff does not send warning letters to entities already under investigation.

[22] Nor does the fact that, in addition to injunctive relief, the court also required Accusearch to disgorge its ill-gotten profits demonstrate that its violations are unlikely to recur. Indeed, when the Commission shows that the law has been violated, the court may use the full range of its equitable authority to remedy the violation and to prevent recurrence. *FTC v. Security Rare Coin & Bullion Corp.*, 931 F.2d 1312, 1314

B. The injunctive relief does not violate the Constitution

There is no merit to any of Accusearch's constitutional arguments. First, its free speech rights are not violated. *See* Br. at 62. To the extent that the First Amendment is implicated at all, it is only the protection for commercial speech. *See U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1233 n.4 (10th Cir. 1999) (expression related solely to the economic interests of the speaker and its audience is commercial speech); *Trans Union Corp. v. FTC*, 267 F.3d 1138, 1140 (D.C. Cir. 2001) (same). Accusearch mistakenly assumes that commercial speech is entitled to absolute constitutional protection. *See* Br. at 57, 62. In fact, as this Court has recognized, the Supreme Court has set forth a three-part test to determine whether a restriction of non-misleading commercial speech violates the First Amendment. *U.S. West*, 182 F.3d at 1233, citing *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm. of New York*, 447 U.S. 557 (1980). First, the government must have imposed the restriction to further a substantial interest. Second, the restriction must directly and materially advance that interest. Third, the restriction must be no more extensive than necessary to further that interest.

The injunctive relief imposed by the court passes the first part of the test because it seeks to further a substantial interest: protecting the privacy of sensitive

---

(8th Cir. 1991); *FTC v. Amy Travel Service, Inc.*, 875 F.2d 564, 571 (7th Cir. 1989); *FTC v. U.S. Oil & Gas Corp.*, 748 F.2d 1431, 1434 (11th Cir. 1984); *FTC v. H.N. Singer, Inc.*, 668 F.2d 1107 (9th Cir. 1982).

consumer information, and keeping that information out of the hands of unauthorized third parties, such as abusers and stalkers. As this Court explained in *U.S. West*, where, as here, the government has shown that the release of information may lead to abuse and harassment, the government's privacy interest is substantial. 182 F.3d at 1235. Second, the restrictions imposed by the district court directly further the government's interest because they prevent abusers and stalkers from obtaining easy access to confidential information regarding their prey. This case is very different from *U.S. West*, where there was no evidence that harm to privacy would actually occur. 182 F.3d at 1237. Here, the Commission presented ample evidence that, as a result of Accusearch's practices, substantial harm had occurred, or was likely to occur, including abuse and stalking. The Commission has also shown that Accusearch caused economic loss and substantial emotional injury. Third, the restrictions imposed by the injunction are narrowly tailored because they prevent the very sorts of privacy infringements that result in the harm the Commission seeks to prevent. Accusearch incorrectly contends that the injunction would prevent it from selling any consumer information. *See* Br. at 17, 56. To the contrary, the court's order specifically permits Accusearch to obtain and sell consumer personal information if that information was lawfully obtained, or if the consumer consented to the sale. *See* D.132 at 3-4. That is, Accusearch is only prohibited from selling information that has been illegally obtained, or without consent. Thus, the injunctive relief is narrowly

tailored -- indeed, it is hard to imagine how it could possibly be more narrowly tailored. Because the relief satisfies all three parts of the *Central Hudson* test, it does not interfere with Accusearch's First Amendment rights.

Nor has Accusearch shown any violation of its Fifth Amendment due process rights. *See* Br. at 53-56. It mistakenly contends that the injunction must be limited to telephone records. In fact, the Supreme Court has made clear that a law violator should expect broad injunctive relief:

> As we said in *FTC v. Ruberoid Co.*, 343 U.S. 470, 473 (1952), "[T]he Commission is not limited to prohibiting the illegal practice in the precise form in which it is found to have existed in the past." Having been caught violating the [FTC] Act, respondents "must expect some fencing in." *FTC v. National Lead Co.*, 352 U.S. 419, 431 (1957).

FTC v. Colgate-Palmolive Co., 380 U.S. 374, 395 (1965). Here, the injunction prohibits Accusearch from selling illegally obtained telephone records and any other illegally obtained consumer personal information. That is, the injunction prohibits Accusearch from engaging in the same type of unlawful conduct that it employed in the past. Given the ease with which Accusearch could apply its unlawful techniques to other consumer information (*i.e.*, protected bank records, or protected health information), the court properly applied the injuction to such conduct.[23]

---

[23] *CPC Int'l, Inc. v. Skippy Inc.*, 214 F.3d 456 (4th Cir. 2000), does not help Accusearch. *See* Br. at 54. In that case, CPC, which markets Skippy peanut butter, sued Skippy Inc., for trademark infringement. Skippy Inc., owned the rights to a cartoon character named Skippy. Skippy Inc., had attempted to license the cartoon character and the Skippy name to a marketer of caramel corn, popcorn, and nuts.

Accusearch cites *NAACP v. Claiborne Hardware Co.*, 458 U.S. 886 (1982), to support the proposition that an injunction must restrain only unlawful conduct. Br. at 54. Of course, that is exactly what the injunction here does -- it only prohibits Accusearch from selling information that it has not been obtained lawfully or with the consumer's consent. Moreover, *Claiborne Hardware* involved an injunction that prohibited conduct that was entitled to full First Amendment protection. *Id.* at 924. Here, as explained above, the conduct to which the injunction applies is subject to the intermediate commercial speech standard. The injunction easily passes that standard. *See supra*. Thus, there is no merit to Accusearch's due process challenge.

Finally, Accusearch mistakenly contends that the district court's injunction somehow violates its right to equal protection under the laws. In particular, Accusearch contends that other entities that were prosecuted by the Commission received less stringent treatment than it did. *See* Br. at 18, 57-58. However, it is well settled that "some selectivity in enforcement is not in itself a federal constitutional violation so long as the selection was not deliberately based upon an unjustifiable

---

Plaintiff CPC prevailed and the court entered an injunction prohibiting Skippy Inc., from licensing its name or the character for use on caramel corn, any peanut product, or *any other food product*. Although the court of appeals cautioned that injunctions must be narrowly tailored, it did so only after the district court attempted to enforce the injunction against a website posted by Skippy Inc., on which it argued that it had been bullied by CPC. However, there was no indication in the case that the provision in the original injunction, which prohibited Skippy, Inc., from licensing its name for any food, posed any problem. The injunction here is no broader than the injunction in *CPC v. Skippy*.

standard such as race, religion, or other arbitrary classification." *Potter v. Murray City*, 760 F.2d 1065, 1071 (10th Cir. 1985); *see United States v. Amon*, 669 F.2d 1351, 1355 (10th Cir. 1981) (same). Indeed, selective prosecution constitutes a violation of the Constitution only if the defendant can establish that the government acted with bad intent, that the defendant is a member of a constitutionally protected class, and that others outside that class were not prosecuted. *Fog Cutter Capital Group Inc. v. SEC*, 474 F.3d 822, 826-27 (D.C. Cir. 2007). Accusearch can show none of these factors: indeed, it has never alleged that the Commission acted with any sort of bad intent. Accordingly, this constitutional argument, like the others, fails.[24]

[24] In connection with its equal protection argument, Accusearch complains that the Commission submitted a declaration to the district court that, according to Accusearch, contained inaccurate information. That declaration addresses the status of several other companies that sold personal information and that had been prosecuted by the Commission. Br. at 57-58. The declarant, Ms. Tracy Thorleifson, explains that those companies had become inactive. Accusearch challenges that declaration based on an inference -- because it can locate a company's website, it infers that the company must be active. Appx. 1533. In fact, as Ms. Thorleifson's Declaration explains, the mere fact that it is possible to locate a company's website on the internet does not establish that the company remains in business, or that, even if it is in business, it has not altered its business. Appx. 1595-97. In any event, because Accusearch cannot show that it is a member of a protected class, the status of other companies prosecuted by the Commission is irrelevant to Accusearch's equal protection argument (and to every other argument that it has raised before this Court).

CONCLUSION

For the reasons set forth above, this Court should affirm the district court's decision.

Respectfully submitted,

WILLIAM BLUMENTHAL
General Counsel

JOHN F. DALY
Deputy General Counsel for Litigation

s/ Lawrence DeMille-Wagman

OF COUNSEL:
TRACY S. THORLEIFSON
KIAL S. YOUNG
Federal Trade Commission
Seattle, Washington

LAWRENCE DeMILLE-WAGMAN
Attorney
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580
(202) 326-2448
lwagman@ftc.gov

STATEMENT REGARDING ORAL ARGUMENT

The Commission believes that the issues in this case were correctly resolved by the district court, and are adequately addressed by the parties' briefs. Nonetheless, the Commission also believes that this Court's understanding of the issues could benefit from argument. Accordingly, the Commission requests oral argument.

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with Fed. R. App. P. 32(a)(7)(B). It is proportionally spaced and contains 13316 words, as counted by the WordPerfect word processing program.

CERTIFICATION OF DIGITAL SUBMISSION

1) I certify that it was not necessary to make any privacy redactions from this brief.

2) I certify that this brief has been scanned for viruses with Symantec AntiVirus Version 6/4/08 rev. 3, and that, according to this program, it is virus-free.

CERTIFICATE OF SERVICE

I hereby certify that on June 6, 2008, I submitted an electronic version of appellee's brief to this Court and to counsel for appellants. Within two business days, I sent one signed original and seven copies of that brief to the Clerk of this Court by express overnight delivery. On the same date I served two copies of the brief on appellants by sending those copies by express overnight delivery to:

Gay Woodhouse
Deborah L. Roden
P.O. Box 1888
211 West 19th Street, 3d Floor
Cheyenne, Wyoming 82003

s/Lawrence DeMille-Wagman

LAWRENCE DEMILLE-WAGMAN
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580
(202) 326-2448
lwagman@ftc.gov