United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued September 10, 2008 Decided February 13, 2009

No. 07-1312

NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION,
PETITIONER

v.

FEDERAL COMMUNICATIONS COMMISSION AND UNITED STATES OF AMERICA,
RESPONDENTS

QWEST COMMUNICATIONS INTERNATIONAL INC. AND VERIZON,
INTERVENORS

On Petition for Review of an Order
of the Federal Communications Commission

Matthew A. Brill argued the cause for petitioner. With him on the briefs were *J. Scott Ballenger*, *Melissa B. Arbus*, *Daniel L. Brenner*, *Neal M. Goldberg*, and *Loretta P. Polk*.

Helgi C. Walker argued the cause for intervenors. With her on the brief were *Andrew G. McBride*, *Brett A. Shumate*, *Michael E. Glover*, *Karen Zacharia*, and *Robert B. McKenna Jr.*.

Joel Marcus, Counsel, Federal Communications Commission, argued the cause for respondents. With him on the brief were *Thomas O. Barnett*, Assistant Attorney General, U.S. Department of Justice, *Catherine G. O'Sullivan* and *Nancy C. Garrison*, Attorneys, *Matthew B. Berry*, General Counsel, Federal Communications Commission, *Joseph R. Palmore*, Deputy General Counsel, and *Richard K. Welch*, Acting Deputy Associate Counsel.

Before: RANDOLPH, ROGERS and TATEL, *Circuit Judges*.

Opinion for the Court filed by *Circuit Judge* RANDOLPH.

RANDOLPH, *Circuit Judge*: Whenever someone makes a call on a telephone or a cell phone, that person's telecommunications carrier receives information about who was called, when, and for how long. Carriers also have records about the kinds of services and features their customers purchase. More than twenty years ago, the Federal Communications Commission required carriers to maintain the confidentiality of such information if their customers so requested. *In re Furnishing of Customer Premises Equipment and Enhanced Services by American Telephone & Telegraph Co.*, 102 F.C.C.2d 655, ¶¶ 64–67 (1985). The Telecommunications Act of 1996 also imposed on carriers a "duty to protect the confidentiality of proprietary information of . . . consumers." 47 U.S.C. § 222(a). Although § 222 permitted carriers to use customer information within the confines of the existing service relationship, it prohibited carriers from otherwise using, disclosing or allowing access to such information except "as required by law" or "with the approval of the customer." *Id.* § 222(c)(1). The issues presented in this petition for judicial review deal with the validity of the Commission's latest order specifying how carriers are to obtain their customers' approval.

I.

Under the 1996 Act, "customer proprietary network information" consists of information relating 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." 47 U.S.C. § 222(h)(1). This statutory definition of what we will refer to as "customer information" encompasses customers' particular calling plans and special features, the pricing and terms of their contracts for those services, and details about who they call and when. Some carriers may use this information to market specific services or upgrades to their customers, tailored to individual usage patterns. Other carriers, especially smaller ones and new market entrants, may find it more efficient to enter into agreements with joint venturers or independent contractors to conduct such targeted marketing.

In its 1998 Order implementing the confidentiality mandate of the 1996 Act, the Commission interpreted § 222 as setting out two categories of uses of customer information: those uses to which customers implicitly consent simply by subscribing to a carrier's services, and those for which the carrier would have to obtain express customer approval. *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 13 F.C.C.R. 8061, ¶ 23 (1998) ("1998 Order"). To delineate the bounds of implicit customer approval, the Commission adopted the "total service approach," which turned on a distinction between three traditional categories of telecommunications services: local telephone service, interexchange (primarily long distance calling service), and commercial mobile radio services (primarily mobile or cellular phone service). *Id.* ¶¶ 24, 27; *see also* 47 C.F.R. § 64.2005(a). The 1998 Order provided that carriers could infer customer approval within the confines of existing service in one or more of the categories above. 1998 Order ¶ 25. Implicit approval also extended to customer information sharing with carriers' affiliates who provide one of the other service types within the existing service relationship between the customer and the carrier. *Id.* ¶ 51. But if carriers wished to use or disclose customer information outside of the existing relationship, even in communications with their customers, the Commission determined that customers had to consent, affirmatively and explicitly, ahead of time. *Id.* ¶ 87. This approach became known as the "opt-in" method.

In *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999), the court of appeals held that the 1998 Order's opt-in consent requirement amounted to an unconstitutional restriction on the carriers' First Amendment right to speak to their customers. *Id.* at 1240. Relying on *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*, 447 U.S. 557 (1980), the court ruled that the Commission had not satisfied "its burden of showing that the customer approval regulations restrict no more speech than necessary to serve the asserted state interests." *U.S. West*, 182 F.3d at 1239. The court cited a lack of evidence that "customers do not want carriers to use their" information; even if there were such evidence, the court thought the Commission had failed to show "that an opt-out strategy would not sufficiently protect consumer privacy." *Id.*

In response to the Tenth Circuit's decision, the Commission initiated a new rulemaking proceeding and issued an order modifying its regulations. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 17 F.C.C.R. 14860 (2002) ("2002 Order"). The Commission stated that "in light of *U.S. West* we now conclude that an opt-in rule for intra-company use [between a carrier and its affiliates] cannot be justified based on the record we have before us." *Id.* ¶ 31. The Commission took into account customers' interest in learning of their carriers' service offerings and what it perceived as a lower risk of infringement of personal privacy when customer information is shared within an organization. The Commission therefore required only opt-out approval for the sharing of customer information between a carrier and its affiliates for communications-related purposes. *Id.* ¶¶ 33–40. The Commission prescribed the content, form, and frequency of the notice and opt-out process, pursuant to which the approval of customers would be presumed unless they specifically told their carriers not to share the information. *Id.* ¶¶ 41, 43, 89–106.

The 2002 Order also allowed carriers to share customer information with joint venture partners or independent contractors for marketing communications-related services. 2002 Order ¶¶ 47–49. But the Commission recognized a heightened personal privacy risk associated with these third parties because they did not qualify as "carriers" under the Telecommunications Act and thus were not subject to § 222's confidentiality requirements. *Id.* ¶ 46. The Commission therefore ordered carriers and their joint venture partners or independent contractors to enter into confidentiality agreements to safeguard customer information, in addition to the opt-out notices sent to customers. *Id.* ¶ 47. Carriers were apparently content with this state of affairs; no challenges were mounted against the 2002 Order.

The Electronic Privacy Information Center petitioned in 2005 for further rulemaking to modify the Commission's customer information sharing rules. The petition noted the increasing number of "data brokers" – organizations that sell private information about individuals online – and expressed concern about how easily these organizations are able to obtain the information from carriers and other entities. Pet. for Rulemaking at 5–8. The petition suggested that data brokers might obtain the information from customer service representatives by pretending to have proper authority to receive it (known as "pretexting"), by gaining unauthorized access to consumers' online accounts with carriers (by hacking, for example), or through "dishonest insiders" working for the carriers. *Id.* at 1. Concerned that inadequate privacy protections contributed to the data broker problem, the Commission initiated a new rulemaking proceeding, received comments, and issued the Order at issue in this case. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 22 F.C.C.R. 6927 (2007) ("2007 Order").

Two months before the Commission adopted the 2007 Order, Congress passed the Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, 120 Stat. 3568 (codified at 18 U.S.C. § 1039). The statute imposed criminal penalties for pretexting, 18 U.S.C. § 1039(a)(1)–(3); unauthorized access to consumer accounts online, *id.* § 1039(a)(4); selling or transferring customer information, presumably by either data brokers or dishonest company insiders, *id.* § 1039(b); and knowing purchase or receipt of fraudulently obtained customer information, *id.* § 1039(c). Congress found that unauthorized disclosure of customer information "not only assaults individual privacy but, in some instances, may further acts of domestic violence or stalking, compromise the personal safety of law enforcement officers, their families, victims of crime, witnesses, or confidential informants, and undermine the integrity of law enforcement investigations." Telephone Records and Privacy Protection Act § 2(5).

In its 2007 Order the Commission changed, for the third time, its requirements for the form of customer approval necessary to satisfy 47 U.S.C. § 222. Relying on "new circumstances" to justify its altered approach, the Commission now required carriers to "obtain opt-in consent from a customer before disclosing that customer's [information] to a carrier's joint venture partner or independent contractor for the purpose of marketing communications-related services to that customer." 2007 Order ¶ 37. The Commission distinguished joint venture partners and independent contractors from affiliates for two reasons. First, it determined that information shared with third-party marketers is subject to a greater risk of loss once out of the carrier's actual control; and second, it determined that those third parties would not likely be subject to the confidentiality requirements of § 222 because they are not themselves carriers. *Id.* ¶ 39. It would not sufficiently protect consumer privacy, the Commission found, for carriers simply to terminate their relationships with third parties who lose customer information, or for the Commission to rely on enforcement proceedings in the case of unauthorized disclosure: at that point, the damage has already been done. *Id.* ¶ 42. The Commission also found, based on studies brought to its attention during the rulemaking process, that consumers were less amenable to the sharing of their private information with third parties without their express prior authorization. *Id.* ¶ 40. It thus concluded that before carriers could share customer information with joint venture partners or independent contractors, the customers had to consent expressly to such sharing. *Id.* ¶¶ 39, 45.

II

Petitioner and intervenors (collectively, "petitioners") think the 2007 Order violates the First Amendment to the Constitution, or is arbitrary in violation of the Administrative Procedure Act, or both. Whatever the heading, their argument is basically the same – that the administrative record does not support the Commission's Order. There is nothing to this.

Before we get to the record we need to be precise about petitioners' position. They have not even attempted to mount an argument that the 2007 Order misinterprets § 222 and so we will assume that the Commission has faithfully adhered to the statute. Nor have they claimed that § 222 violates the First Amendment, or that it is arbitrary or capricious. The question naturally arises: if the First Amendment did not bar Congress (in § 222) from requiring carriers to obtain their customers' consent, how can it be that the First Amendment bars the Commission from implementing § 222 by requiring customer consent? Petitioners give this answer: "Both the First Amendment and the Administrative Procedure Act . . . require that the Commission . . . support its assertions with *evidence* before it may restrict the communication of truthful, lawfully obtained information between carriers and their marketing partners, and the ways that carriers may communicate with their existing customers." Pet'r Br. 19–20 (emphasis in original). They say this evidence is needed because the "selective opt-in requirement" is more restrictive than the opt-out system it replaced. *Id.* at 20.

It is true that in some First Amendment cases the Supreme Court has demanded an evidentiary showing in support of a state's law. *See, e.g.*, *Turner Broad. Sys., Inc. v. FCC*, 520 U.S. 180, 195 (1997); *Edenfield v. Fane*, 507 U.S. 761, 770–71 (1993). It is also true that in other First Amendment cases the Supreme Court has found "various unprovable assumptions" sufficient to support the constitutionality of state and federal laws, particularly laws regulating business. *Paris Adult Theater I v. Slaton*, 413 U.S. 49, 61 (1973). But this case comes to us in a different posture. By conceding the constitutionality of § 222, petitioners necessarily concede at least two factual predicates underlying both the statute and the Commission's Order – namely, that the government has a substantial interest in protecting the privacy of customer information and that requiring customer approval advances that interest. We put the matter in these terms because all parties proceed on the basis that what we have here is a regulation of commercial speech, and that the validity of the regulation must therefore be tested according to the standards set forth in *Central Hudson*, 447 U.S. at 566: the speech must "at least concern lawful activity and not be misleading"; the "governmental interest [must be] substantial"; the regulation must "directly advance[] the governmental interest asserted"; and the regulation must not be "more extensive than is necessary to serve that interest." We too will assume that *Central Hudson* controls.

The first part of *Central Hudson* is not in play so we turn to the second – is there a "substantial" governmental interest? Petitioners seem to recognize that they cannot contest the point in light of their agreement that § 222 is constitutional. Pet'r Br. 29. Still, we think it important – particularly in light of the Tenth Circuit's opinion in *U.S. West* – to spell out the nature of the governmental interest at stake. The Tenth Circuit supposed that § 222 sought to promote a governmental interest in protecting against the disclosure of "information [that] could prove embarrassing," and it doubted whether this interest could be deemed "substantial." *U.S. West*, 182 F.3d at 1235. We do not share the Tenth Circuit's doubt. For one thing, we have already held, in an analogous context, that "protecting the privacy of consumer credit information" is a "substantial" governmental interest, as *Central Hudson* uses the term. *Trans Union Corp. v. FTC*, 245 F.3d 809, 818 (D.C. Cir. 2001). For another thing, we do not agree that the interest in protecting customer privacy is confined to preventing embarrassment as the Tenth Circuit thought. There is a good deal more to privacy than that. It is widely accepted that privacy deals with determining for oneself when, how and to whom personal information will be disclosed to others. *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1109–10 (2002). The Supreme Court knows this as well as Congress: "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person." *U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 763 (1989).*

The next question that must be posed under *Central Hudson* is whether the Commission's 2007 Order "directly advances" the governmental interest just identified. Here again petitioners' agreement that § 222 complies with the First Amendment all but settles the issue. The privacy of customer information cannot be preserved unless there are restrictions on the carrier's disclosure of it. *See Trans Union Corp. v. FTC* (*Trans Union II*), 267 F.3d 1138, 1142 (D.C. Cir. 2001), *denying reh'g in* 245 F.3d 809 (D.C. Cir. 2001). And the restriction Congress imposed was customer approval. But petitioners say the Commission violated the First Amendment by implementing this congressional requirement with an opt-in system. According to petitioners, the record does not indicate that joint venturers or independent contractors have disclosed customer information to others. Pet'r

* After the *U.S. West* decision, when Congress criminalized unauthorized disclosure of customer information, it found that "the unauthorized disclosure of telephone records not only assaults individual privacy but, in some instances, may further acts of domestic violence or stalking, compromise the personal safety of law enforcement officers, their families, victims of crime, witnesses, or confidential informants, and undermine the integrity of law enforcement investigations." Telephone Records and Privacy Protection Act § 2(5). The Commission relied on these and related Congressional findings in its 2007 Order, *e.g.*, 2007 Order ¶ 44, and it also learned of specific incidents that confirmed some of the dangers Congress enumerated, *id.* ¶ 12 n.31.

Br. 30. This argument, by focusing on what happens after a joint venturer or independent contractor receives the information, performs a sort of sleight of hand. It diverts attention from the fact that the carrier's sharing of customer information with a joint venturer or an independent contractor without the customer's consent is itself an invasion of the customer's privacy – the very harm the regulation targets. In addition, common sense supports the Commission's determination that the risk of unauthorized disclosure of customer information increases with the number of entities possessing it. The Commission therefore reasonably concluded that an opt-in consent requirement directly and materially advanced the interests in protecting customer privacy and in ensuring customer control over the information. The 2007 Order's "means and ends are thus one," *Trans Union II*, 267 F.3d at 1143.

This brings us to *Central Hudson*'s final requirement that the restriction on commercial speech must be "no more broad or no more expansive than necessary to serve its substantial interests." *Bd. of Trs. of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 476 (1989) (internal quotation marks omitted). The government does not have to show that it has adopted the least restrictive means for bringing about its regulatory objective; it does not have to demonstrate a perfect means–ends fit; and it does not have to satisfy a court that it has chosen the best conceivable option. *Id.* at 476–81. The only condition is that the regulation be proportionate to the interests sought to be advanced. *Id.* at 480; *see also Fla. Bar v. Went For It, Inc.*, 515 U.S. 618, 632 (1995). The 2007 Order easily meets this standard.

The Commission's opt-in consent scheme presumes that consumers do not want their information shared unless they expressly indicate otherwise; an opt-out scheme, which is what petitioners want, presumes the opposite. Confronted with a challenge analogous to this one, we held that opt-out is only "'marginally less intrusive'" than opt-in for First Amendment purposes and so upheld a nearly identical regime requiring opt-in consent for the sharing of customer credit information. *Trans Union II*, 267 F.3d at 1143 (quoting *Turner Broad. Sys.*, 520 U.S. at 217–18). In that case we did not require exhaustive evidence documenting the necessity of opt-in over opt-out; we relied on Congress's reasonable, commonsense determination that express customer consent was required. In any event, here the Commission carefully considered the differences between these two regulatory approaches, and the evidence supports the Commission's decision to prefer opt-in consent. Unlike the 1998 Order at issue in *U.S. West*, the 2007 Order required opt-in consent only with respect to a carrier's sharing of customer information with third-party marketers. The evidence showed that customers were less willing to have their information shared with third parties as opposed to affiliated entities. And the Commission reasonably concluded that customer information would be at a greater risk of disclosure once out of the control of the carriers and in the hands of entities not subject to § 222. Contractual safeguards requiring the carrier to terminate its relationship with the third party after a breach – a solution carriers favored – would not sufficiently protect customer privacy because, the Commission stated, "the damage is already inflicted upon the customer." 2007 Order ¶ 42.

III

Petitioners' claim under the Administrative Procedure Act, 5 U.S.C. § 706(2)(A), fails for the same reasons we reject their First Amendment claim: substantial evidence supported the Commission's 2007 Order and its reasoning cannot be faulted. There is one wrinkle in administrative law that petitioners seek to use to their advantage. When an agency departs from its previous policy, it must give a "reasoned analysis" for the change. *See Motor Vehicle Mfrs. Ass'n of U.S. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 42 (1983). The argument is that the Commission acted arbitarily when, in light of evidence of unauthorized disclosures by *carriers*, it reversed the policy of its 2002 Order and imposed greater restrictions on the carriers' sharing of customer information with third-party marketing partners. Intervenors' Br. 25.

Petitioners think *National Fuel Gas Supply Corp. v. FERC*, 468 F.3d 831 (D.C. Cir. 2006), supports their position. We think not. In *National Fuel*, 468 F.3d at 833, the Federal Energy Regulatory Commission extended Standards of Conduct that applied to commercial relationships between natural gas pipelines and their marketing affiliates to apply equally to the pipelines' non-marketing affiliates, such as producers, gatherers, processors, and traders. The court held that, to justify this extension of the Standards, the Commission had to present evidence of the *kinds* of abuses that could occur between pipelines and their affiliates who did not perform marketing services. *Id.* at 841. Evidence of abuses between pipelines and marketing affiliates, being different in kind from the abuses that would occur with non-marketing affiliates, could not justify a regulation imposed on those non-marketing affiliate relationships. *Id.* at 842. In contrast, here the governmental interest and potential harms are the same for customer information in the hands of carriers, affiliates, or third-party marketing partners. The Commission explained that customer information could be illegally obtained by the same methods from any organization, regardless of the nature of the entity.

Accordingly, because the Commission returned to a limited opt-in consent requirement in response to the increasing activity of data brokers, and because it gave sufficient reasons for singling out the relationships between carriers and third-party marketing partners, we hold that the Commission adequately provided the reasoned analysis *State Farm* requires.

The petition for judicial review is denied.