VOLUME 23 FALL 2017

ILLINOIS BUSINESS LAW JOURNAL

SHARING IS NOT CARING: INTERNET SERVICE PROVIDERS SELLING CUSTOMER DATA WITHOUT CONSENT

❖ NOTE ❖

*Stuart G. Walker**

TABLE OF CONTENTS

I. INTRODUCTION

Jim uses his computer for everything: Shopping, talking to friends, running his business, keeping up with current events, and relaxing while watching YouTube. In the privacy of his own home, he assumes that everything he does on the computer is private. He frequents a website dedicated to managing a medical condition. He visits a website for substance abuse self-help. He visits a car website and looks up a specific model of car. At some point he notices he has started to get spam mail and emails about managing substance abuse, AA groups in his area, and local car dealerships. It cannot be a coincidence. He did not enter any of his personal information on these websites. How could they find his email or address? They didn't, but his Internet Service Provider knew those things all along.

*J.D. Candidate, Class of 2019, University of Illinois College of Law.

People are uneasy about the large amounts of our data that corporations have and how they might be using it. Their concern, however, should be for the significant gaps in regulation of Internet Service Providers (ISPs).[1] Just as Telephone companies connect individuals' telephone calls, ISPs connect internet users to the internet, channeling their requests to access websites.[2] ISPs can share or sell their customers' internet information without consent.[3] This is a result of the Federal Communication Commission (FCC) policy, deficiencies in the Electronic Communications Privacy Act (ECPA) of 1986, and the inability of the FCC and Federal Trade Commission (FTC) to coordinate efforts to regulate the industry while protecting consumers.

This note explores the gap in regulation for ISPs and the likely outcome and privacy effects of recent litigation between the states and the FCC. The discussion will briefly summarize advertising and selling data on the Internet, the privacy limitations of ISPs, and administrative agencies responsible for regulating ISPs. Then the discussion will proceed and analyze recent litigation considering case law and its likely effect on ISP privacy regulation. Finally, this note will recommend a possible solution that balances business and user privacy interests.

II. BACKGROUND

ISPs have complete access to their user's web information. All user internet traffic passes through ISPs.[4] Like a telephone company switchboard, an ISP directs requests for webpages, and transmits the content back to the user.[5] An ISP creates a record of every webpage the user visits as well as uploaded information such as YouTube videos, tweets, Facebook, instant messages, downloaded music, images,

---

[1] ISP's include Comcast, AT&T, Cox Communications, Time Warner Cable and Charter, to name a few.
[2] Tim Fischer, *Internet Service Provider (ISP) What Exactly Does An Internet Service Provider Do?*, LIFEWIRE (Dec. 1, 2017), https://www.lifewire.com/internet-service-provider-isp-2625924.
[3] Jon Brodkin, *How Isps Can Sell Your Web History—And How To Stop Them,* ARS TECHNICA (Mar. 24, 2017, 11:20 AM), https://arstechnica.com/information-technology/2017/03/how-isps-can-sell-your-web-history-and-how-to-stop-them/.
[4] Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, U. ILL. L. REV. 1417, 1423 (2009).
[5] *Cf. Id.*

and emails.[6] ISPs' raw records include when users are online, where users are when they connect to the Internet, and how often users visit websites. All of this constitutes user information.[7] It can reveal an abundance of information about user habits.[8] For example, if a user looked up an abortion website, visited a planned parenthood website, accessed dcabortionfund.org, and then visited google maps, all within an hour, one could reasonably conclude the user was planning to have an abortion, was female, in the Washington D.C. area, and needed help paying for an abortion.[9]

ISPs can sell this wealth of raw information to marketing and data companies, generating revenue beyond their users' internet subscription fees.[10] Online advertising is a major source of revenue for internet companies.[11] This is because advertisements are more effective when they are tailored to the web users,[12] since consumers are more likely to buy products that are targeted at them.[13]

---

[6] *Id*. at 1438–39 ("It includes a replica copy of every web page visited and every e-mail message sent or received. It includes every instant message, video download, tweet, Facebook update, file transfer, VoIP conversation, and more.").

[7] "Information" is a general term. ISPs have subscribers information relating to their accounts such as names, billing information, addresses, service packages, IP addresses, web addresses visited, browser types like Chrome, Mozilla, Edge, as well as time, location, file size, and transmitted file names and many other pieces of information. *See generally*, *What ISPs Can See*, UPTURN (Mar. 2016), https://www.teamupturn.org/reports/2016/what-isps-can-see, (last visited Feb. 2, 2018).

[8] Darlene Storm, *What Can Your ISP Really See And Know About You?*, COMPUTER WORLD (Mar 14, 2016, 10:53 AM), https://www.computerworld.com/article/3043490/security/what-can-your-isp-really-see-and-know-about-you.html.

[9] *Id*.

[10] Rani Molla, *ISPs Could Lose a Data Gold Mine*, BLOOMBERG: GLADFLY, (April 7, 2016, 8:00 AM), https://www.bloomberg.com/gadfly/articles/2016-04-07/fcc-rules-could-hurt-isp-data-mining.

[11] *See* Nathaniel Gleicher, *Neither A Customer Nor A Subscriber Be: Regulating the Release of User Information on the World Wide Web*, 118 YALE L.J. 1945, 1948–49 (2009); Jay P. Kesan, Carol M. Hayes and Masooda N. Bashir, *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH & LEE L. REV. 341, 346 (2013).

[12] Kesan et al., *supra* note 11.

[13] *See* Jacob B. Hirsh, *Marketing Is More Effective When Targeted to Personality Profiles*, ASSOCIATION FOR PSYCHOL. SCI. (May 21, 2012), https://www.psychologicalscience.org/news/releases/marketing-is-more-effective-when-targeted-to-personality-profiles.html.

Tailored or customized advertising depends on collecting and storing information[14] about users' habits or characteristics and presenting advertisements in a way that fits their interests.[15] Data brokers buy customer information from ISPs, and then aggregate it to create collections of detailed profiles of people.[16] Then they may sell the profiles to anyone including the government or law enforcement.[17]

There are significant privacy concerns in ISP data collection and storage because ISPs are exempt from major parts of privacy laws. Much of the basis of online privacy policy for ISPs involves the Electronic Communications Privacy Act of 1986 (ECPA).[18] The ECPA includes protection for stored and transmitted communications as well as guidelines for disclosure of the content of the communications.[19] Storage is specifically covered under The Stored Communication Act (SCA), which "punishes the intentional unauthorized … access to a wire or electronic communication while it is in electronic storage…."[20] The SCA, however, excludes actions by ISPs regarding stored communications as conduct authorized "by the person or entity providing a wire or electronic communications service."[21] The SCA allows voluntary disclosure of any and all non-content user information by an ISP, "to any person other than a governmental entity."[22]

Courts have interpreted the SCA and ECPA to give the most protection to email content and less protection to consumer account information like web browser records. Courts hold "content" to mean "the substance, purport, or meaning

---

[14] Gleicher, *supra* note 11.
[15] *See*, Rebecca Walker Reczek, Christopher Summers, Robert Smith, *Targeted Ads Don't Just Make You More Likely to Buy — They Can Change How You Think About Yourself*, HARV. BUS. REV. (Apr. 04, 2016), https://hbr.org/2016/04/targeted-ads-dont-just-make-you-more-likely-to-buy-they-can-change-how-you-think-about-yourself.
[16] *Cf.*, *Data Brokers And "People Search" Sites*, PRIVACY RIGHTS CLEARINGHOUSE (Oct 17, 2017), https://www.privacyrights.org/consumer-guides/data-brokers-and-people-search-sites.
[17] *Id.*
[18] 18 U.S.C. §§ 2510-2522, 2701–2712 (2012).
[19] *Id.*
[20] 18 U.S.C. § 2701 (2012); *see* §§ 2701–2712 (2012).
[21] *Id.* § 2701.
[22] 18 U.S.C. § 2702(c)(6) (2012).

of [the] communication"[23] including the written portions of emails,[24] texts,[25] and email subject lines.[26] Non-content includes information such as customer account information and metadata including user location,[27] IP address,[28] web address,[29] email recipient,[30] and possibly even search terms.[31]

Consumers cannot avoid collection and sale of their data even if they switch to a smaller ISP or attempt to sacrifice speed for privacy by using an ISP that provides slower internet speeds. Even if switching to a different ISP was a solution, internet users do not have many choices of ISP providers. In 2015, the FCC reported that eighty percent of US Census blocks[32] had access to one or fewer internet providers.[33] In 2017, around 100 million Americans had no choice but to get broadband from an ISP that violated Net Neutrality.[34] Thus, many Americans have no choice but to sacrifice their privacy for use of the Internet.

---

[23] 18 U.S.C. §2510(8) (2012).
[24] Quon v. Arch Wireless Operating Co., Inc., 445 F. Supp. 2d 1116, 1135 (C.D. Cal. 2006).
[25] *E.g.*, Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 910 (9th Cir. 2008).
[26] Graf v. Zynga Game Network, Inc. (In re Zynga Privacy Litig.), 750 F.3d 1098, 1106 (9th Cir. 2014).
[27] *See*, Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 305-06 (3d Cir. 2010) (considering cell phone location data to be non-content).
[28] *Graf,* 750 F.3d at 1104.
[29] *Cf.*, *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 139 (3d Cir. 2015) (arguing that in a special case some URLs might qualify as content. This implicitly acknowledges that generally URLs are not content.).
[30] *Graf*, 750 F.3d at 1107.
[31] *In re Google*, 806 F.3d at 137.
[32] *Geographic Terms and Concepts – Block,* UNITED STATES CENSUS BUREAU https://www.census.gov/geo/reference/gtc/gtc_block.html (defining Block as small geographic areas divided by the number of people present; used to uniformly group people for the census) (last visited Jan. 18, 2018).
[33] Jon Brodkin, *US Broadband: Still No ISP Choice For Many, Especially At Higher Speeds*, ARS TECHNICA (Aug. 10, 2016, 10:43 AM), https://arstechnica.com/information-technology/2016/08/us-broadband-still-no-isp-choice-for-many-especially-at-higher-speeds/.
[34] Kaleigh Rogers, *More than 100 Million Americans Can Only Get Internet Service from Companies That Have Violated Net Neutrality*, VICE: MOTHERBOARD (Dec. 11, 2017, 1:30 PM), https://motherboard.vice.com/en_us/article/bjdjd4/100-million-americans-only-have-one-isp-option-internet-broadband-net-neutrality (using a liberally broad definition of 'net neutrality violation' to mean behaviors that are opposed to it, including politically opposing net neutrality, all the way to actually throttling back on internet speeds).

The FCC is the administrative agency responsible for regulation of ISPs. The FCC's authority over ISPs was legislated by the Telecommunications Act of 1996 which modified the existing the Communications Act of 1934.[35] This authority[36] includes the ability to regulate according to ISP designation as a common carrier under Title II, or under § 706 to encourage growth, competition, remove barriers to infrastructure development and overall broadband access to consumers.[37]

Historically, the FCC has done little to regulate ISPs' use of customer information.[38] But in 2016, the FCC ordered privacy protections for customers that would have required ISPs to get customer consent before selling or distributing their customers' information.[39] Then in March 2017, before it could take effect, Congress voted to undo the order.[40] That law further prevents the FCC from attempting to promulgate similar consumer privacy protections against ISP's in the future.[41] On January 4, 2018, the FCC issued an order, *In the Matter of Restoring Internet Freedom,* to declassify ISPs as common carriers, undoing "Net Neutrality"[42] in order to "exercise [the FCC's] forbearance authority to establish a

---

[35] Haran Craig Rashes, *The Impact of Telecommunication Competition and the Telecommunications Act of 1996 on Internet Service Providers*, 16 TEMP. ENVTL. L. & TECH. J. 49, 60 (1997); *see also,* 47 U.S.C. §§ 153, 522 (2012).

[36] 47 U.S.C. § 154 (2012) ("The Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter[5], as may be necessary in the execution of its functions"); *see,* Jim Chen, *The Authority to Regulate Broadband Internet Access Over Cable*, 16 BERKELEY TECH. L.J. 677, 723 (2001).

[37] Verizon v. F.C.C., 740 F.3d 623, 635 (D.C. Cir. 2014), *see also*, 47 U.S.C. §§ 1302(a)–(b) and 706(b).

[38] *Cable Television Privacy Requirements Enter the World of Internet Service Providers,* MEDIA L. & POL'Y, SPG 1997, at 1, 5–6

[39] FCC, NO. 16-106, REPORT AND ORDER: PROTECTING THE PRIVACY OF CUSTOMERS OF BROADBAND AND OTHER TELECOMMUNICATIONS SERVICES (2016); *see also* 47 C.F.R. § 64.

[40] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Pub. L. 115-22, April 3, 2017, 131 Stat 88.

[41] Richard S. Beth, *Disproval of Regulations by Congress: Procedure Under the Congressional Review Act*, CONGRESSIONAL RESEARCH SERVICE (Oct. 10, 2001), at Summary ¶ 2, https://www.senate.gov/CRSpubs/316e2dc1-fc69-43cc-979a-dfc24d784c08.pdf.

[42] *What is Net Neutrality?*, ACLU (Dec. 2017), https://www.aclu.org/issues/free-speech/internet-speech/what-net-neutrality (Net Neutrality is basically a policy to prevent ISPs from controlling or limiting speed or access to websites, or discriminating by selling

'light-touch' regulatory regime"[43] and "return jurisdiction to regulate broadband privacy and data security to the Federal Trade Commission."[44]

Handing authority back to the FTC, as the FCC does in the order, *In the Matter of Restoring Internet Freedom*, is insufficient to protect users' privacy from the brazen and open selling of data. The Federal Trade Commission (FTC) plays a role in enforcing privacy policies by prosecuting companies' use of "unfair or deceptive trade practices" under § 5 of the Federal Trade Commission Act,[45] which includes companies' privacy policies.[46] A privacy policy, even if just a general statement or a non-binding "promise that is offered freely and equally to all people,"[47] can be regulated by the FTC as a false or misleading business practice that induced the user to accept and use the service.[48] This means that the FTC enforces a company's own privacy policies against it, ensuring the company does what it says it will do. The company still decides what, if any, privacy policy to have.[49] This means the FTC is unable to proactively change an ISP's ability to share information so long as the ISP's privacy policy says that it can do so.

The FCC's order, *In the Matter of Restoring Internet Freedom,* produces a gap between the protection users may expect and what the FTC can provide. The FCC implicitly acknowledges this gap when it suggests users must rely on self-help

---

faster internet traffic to sites willing to pay more) (Net Neutrality is not central to the issue of privacy, but the results of Net Neutrality litigation and challenges to FCC preemption may set precedents for other areas, including whether the FCC can preempt state laws regulating ISP privacy policy.).

[43] FCC, *In the Matter of Restoring Internet Freedom,* DECLARATORY RULING, REPORT AND ORDER, AND ORDER, (Adopted: Dec. 14, 2017) (released: Jan. 4, 2018), ¶ 274.

[44] *Id.* ¶181.

[45] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2114 (2004) (internal footnotes and citations omitted).

[46] FEDERAL TRADE COMM'N, *Enforcing Privacy Promises*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises. (last visited Jan. 17, 2018).

[47] Austin-Spearman v. AARP & AARP Servs. Inc., 119 F. Supp. 3d 1, 11–12 (D.D.C. 2015).

[48] FTC, *Enforcing Privacy Promises*, *supra.*; *See generally*, Federal Trade Commission Act, 15 U.S.C. §§ 41 et seq. (2012).

[49] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2114 (2004) (internal footnotes and citations omitted).

measures[50] to protect their privacy from intrusion by their ISPs,[51] while reserving the ability to review the reasonableness of ISP practices on a case-by-case basis.[52]

III. ANALYSIS

The FCC's order *In the Matter of Restoring Internet Freedom,* has not given any meaningful privacy authority to the FTC. The reservation[53] of authority combined with the preemption of state regulation means that any change to ISP practices or protection of ISP user privacy will have to come from Congress, unless the courts disagree with the FCC about preemption.

The FCC order explicitly preempts state legislation that might impair or inhibit ISPs from the view and mission of the FCC.[54] Two states previously passed laws that regulate ISPs' ability to share information without customer consent,[55] while a number of states have internet privacy legislation pending.[56] Twenty-one states including Illinois have filed lawsuits challenging the grounds for preemption.[57] These suits primarily contest the FCC repeal of Net Neutrality,[58] and do not specifically address privacy. Their complaints are grounded either on problems with the Net Neutrality comment process,[59] or they challenge the FCC's

---

[50] *I.e.*: using a VPN, HTTPS, and TOR.
[51] FCC, *In the Matter of Restoring Internet Freedom,* DECLARATORY RULING, REPORT AND ORDER, AND ORDER, (Adopted: Dec. 14, 2017) (released: Jan. 4, 2018) at ¶ 305.
[52] *Id*.
[53] *See id*. at fn. 52.
[54] *Id*. ¶ 194-195. ("[W]e thereby preempt any so-called "economic" or "public utility-type" regulations[.]")
[55] Minn. Stat. §§ 325M.01 to .09; Nevada Revised Stat. § 205.498.
[56] NCSL, *Privacy Legislation Related to Internet Service Providers-2018*, Jan. 29, 2018, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers.aspx.
[57] Jon Brodkin, *21 States Sue FCC To Restore Net Neutrality Rules,* ARS TECHNICA (Jan. 16, 2018, 3:17 PM), https://arstechnica.com/tech-policy/2018/01/21-states-sue-fcc-to-restore-net-neutrality-rules/.
[58] *What is Net Neutrality?*, ACLU, https://www.aclu.org/issues/free-speech/internet-speech/what-net-neutrality (last visited Feb. 2, 2018) (Net Neutrality is basically a policy to prevent ISPs from controlling or limiting speed or access to websites, or discriminating by selling faster internet traffic to sites willing to pay more).
[59] *A.G. Schneiderman: I Will Sue to Stop Illegal Rollback of Net Neutrality*, N.Y. State Office of the Attorney General, press release (Dec. 14, 2017), https://ag.ny.gov/press-release/ag-schneiderman-i-will-sue-stop-illegal-rollback-net-neutrality; *Madigan Will Appeal FCC Vote to Eliminate Net Neutrality Rules*, Illinois State Office of the Attorney

ability to preempt states that wish to introduce Net Neutrality regulation on the state level.[60] The resulting precedent of this litigation will likely affect states' laws regulating ISPs, including internet privacy protection.

The existing case law gives an indication of how this litigation might be decided. In 2004, the Supreme Court held in *Nixon v. Missouri Municipal League*, that the FCC did not have the ability to preempt state regulations that specifically and only targeted the ability of municipal authority to participate the telecommunications market.[61] The case involved a Missouri municipality providing telecommunications services prohibited by Missouri statutes.[62] The FCC did not claim preemptive authority, and according to the *Gregory* rule,[63] such preemptions should be clearly intended by congress. The case interpreted § 253 of the Telecommunications Act, which prevents "any entity" from prohibiting telecommunications service.[64] The Supreme Court held that § 253 did not indicate that "any entity"[65] was intended to apply to matters between a state and its local government,[66] indicating that the FCC's ability to preempt state privacy laws depends on whether the state is regulating public entity and whether the scope is local or interstate.

General, press release (Dec. 14, 2017), http://www.illinoisattorneygeneral.gov/pressroom/2017_12/20171214.html.

[60] *Attorney General Becerra Sues FCC Over Repeal of Net Neutrality Rules,* California State Office of the Attorney General, press release (Jan. 16, 2018), https://oag.ca.gov/news/press-releases/attorney-general-becerra-sues-fcc-over-repeal-net-neutrality-rules; *see also*, Ben Heuso, Mike Morrell, *Re: Federal Communications Commission's December 14, 2017 decision to end oversight over Internet Service Provider industry and its impact on privacy and network neutrality*, ELECTRONIC FRONTIER FOUNDATION (Jan. 11, 2018).

[61] Nixon v. Missouri Mun. League, 541 U.S. 125, 140–41 (2004).

[62] *Id.* at 128–132.

[63] Gregory v. Ashcroft, 501 U.S. 452, 464 (1991) ("[W]e must be absolutely certain that Congress intended such an exercise. '[T]o give the state-displacing weight of federal law to mere congressional *ambiguity* would evade the very procedure for lawmaking on which *Garcia* relied to protect states' interests.'" (citation omitted)).

[64] 47 U.S.C. § 253 (2012) ("No State or local statute or regulation, or other State or local legal requirement, may prohibit or have the effect of prohibiting the ability of any entity to provide any interstate or intrastate telecommunications service.").

[65] *Nixon,* 541 U.S. at 129.

[66] *Id*. at 140.

Ten years later in 2014, the D.C. Circuit Court held in *Verizon v. F.C.C.*, that § 706 was a congressional grant of authority to adopt regulations or take "immediate action" . . . "by removing barriers to infrastructure investment and by promoting competition[.]"[67] Section 706(a)-(b) of the Telecommunications Act indicates, the FCC and states will encourage deployment on a "reasonable and timely basis" of telecommunications with measures that promote development or remove barriers, and further allow that if deployment does not occur in a "reasonable and timely fashion" that the FCC take immediate action to accelerate deployment by removing barriers and promoting competition.[68] Verizon disputed an FCC order to ISPs on transparency practices, prohibiting blocking and "throttling" of internet speed.[69] The court applied the *Chevron* rule[70] and determined that the FCC's order was a reasonable resolution of the ambiguity[71] given the FCC's findings that broadband deployment was not reasonable and timely.[72] This shows that courts are willing to adopt FCC interpretations, at least as they relate to private entities, if the FCC provides a reasonable interpretation of the Telecommunications Act in the scope of an interstate context.

---

[67] Verizon v. F.C.C., 740 F.3d 623, 635, 641 (D.C. Cir. 2014) ("[W]e believe the Commission has reasonably interpreted section 706(b) to empower it to take steps to accelerate broadband deployment if and when it determines that such deployment is not "reasonable and timely.").

[68] *Id.* at 635. (quoting § 706(a) "The Commission and each State commission with regulatory jurisdiction over telecommunications services shall encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans (including, in particular, elementary and secondary schools and classrooms) by utilizing, in a manner consistent with the public interest, convenience, and necessity, price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market, or other regulating methods that remove barriers to infrastructure investment." Quoting § 706(b): "[if] the Commission find that "advanced telecommunications capability is [not] being deployed to all Americans in a reasonable and timely fashion," it "shall take immediate action to accelerate deployment of such capability by removing barriers to infrastructure investment and by promoting competition in the telecommunications market.")

[69] *Id*. at 33–34.

[70] Chevron, U.S.A., Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837 (1984).

[71] *Verizon,* 740 F.3d at 641.

[72] *Id*. at 635 ("[I]f we determine that the Commission's interpretation of section 706 represents a reasonable resolution of a statutory ambiguity, we must defer to that interpretation."); *See also*, *Chevron,* 467 U.S. at 843.

In 2016 the Sixth Circuit Court held in *Tennessee v. Federal Communications Commission*, that under § 706, the FCC did not have power to preempt state regulations prohibiting the expansion of telecommunications operated by municipalities.[73] The court used the *Gregory* rule, but based the reasoning that § 706 shared power between the FCC and state government, specifying that state authority could not trump a municipality's discretion without a clear statement from congress in the statute.[74] The court also limited the scope of its holding to FCC attempts to preempt state regulation over municipalities; it declined, however, to say § 706 had no preemptive power.[75]

These decisions can be unified if courts are acknowledging FCC primacy under a *Chevron* standard in well-reasoned FCC orders over private telecommunications entities operating in an interstate context, and a *Gregory* standard towards state authority over state local government in an intrastate context. The current litigation between the states and the FCC is a fight over who has authority over private entities (ISPs) engaged in interstate Telecommunications. When the regulatory action contemplated by states may have effects to telecommunications that extend interstate, courts will likely interpret Federal regulations to the contrary as having preemptive force.[76] Given the possible negative effects of inconsistent application of Net Neutrality across states, courts would very likely find that the FCC has preemptive authority over states' legislation regarding interstate ISPs.

States that have passed privacy laws affecting ISPs would be open to preemption under this precedent.[77] As more states implement their own privacy laws restricting ISP sale of consumer information on the citizens of that state, it will quickly become difficult for ISPs to comply as internet traffic is being routed

---

[73] Tennessee v. Fed. Commc'ns Comm'n, 832 F.3d 597, 613 (6th Cir. 2016).
[74] *Id*.
[75] *Id.* at 613–14.
[76] *Gregory*, 501 U.S. at 463–64.
[77] Jon Brodkin, *Pressure Grows On FCC To Kill State Consumer Protection Laws,* ARS TECHNICA (Nov. 15, 2017, 12:10 PM), https://arstechnica.com/tech-policy/2017/11/broadband-lobby-steps-up-attack-on-state-privacy-and-net-neutrality-laws/.

through various states as well as make up revenue lost from restrictions on selling data. Future litigation may duplicate *Verizon*, and ISPs will petition the FCC to declare states' privacy requirements on ISPs to be barriers interfering with the interstate goals of § 706, and therefore within the power of the FCC to preempt states' privacy laws as barriers to the growth of broadband. ISP's claims will become stronger as more states implement privacy laws, and if the laws are not uniform between the states.

Ultimately, the current states' cases against the FCC and any state laws that ISPs may litigate as violations of the FCC order, will likely be found in favor of the FCC. The congressional authority placed in the FCC given its granted power to regulate ISPs in the interstate transmission of data over the Internet is clearly under the authority of the FCC. The only way therefore to change the FCC, is through congressional legislation that will update the aged ECPA of 1986.

IV. RECOMMENDATION

The best solution would be legislation updating the ECPA to modern internet-age conceptions of privacy and apply it to all internet entities. Legislation solely targeting ISPs would not balance user privacy interests uniformly beyond ISPs to other internet companies as well. Care must be taken to also account for the importance of advertising and data collection to the revenue of internet services. The difficulty of balancing financial and privacy concerns is one reason why privacy legislation has likely not yet occurred. It is not desirable or financially viable to restrict all data collection, prohibit data sales, or advertising. Doing so may chill or restrict the growth of internet infrastructure as the FCC claims, or stop internet company startups or the dissemination of free applications and programs.

Drawing a line might be palatable if the line were "customizable" by individual users on a continuum and configured to favor business interests with a "low privacy" default setting. But like the "Do Not Call" list,[78] individuals must opt-in to get the benefit of additional privacy. The privacy settings would have to be protected, meaning that companies could not discriminate against users (slowing

[78] *See* Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227(c) (2012).

connections, denying service) because one opted into more privacy. Companies would be prohibited from attempting to require that users "waive" their privacy settings in order to nullify the user's privacy on their service.

Psychological studies have shown the effect of default settings in employee 401k contributions,[79] and therefore one could assume that most internet users would not change their settings. Users that don't care about their privacy won't touch their default settings, while those that do care would opt for the highest settings. This would preserve the revenue generating potential of internet data collection while allowing improvements in privacy to those that care enough to opt into higher settings on an internet privacy continuum.

Such legislation would put meaningful privacy control in the users' hands and allow them to control what information is collected and sold, while balancing the financial concerns of companies such as ISPs and internet companies.

V. CONCLUSION

In conclusion, the current privacy laws are insufficient for regulating ISPs data sharing. The current FCC and FTC agencies are equally unable to require ISPs to engage in or guarantee data sharing practices that allow the user control of their information, or prevent its sale. Based on recent regulatory actions and court history, state legislation may be preempted by the FCC. The only way the situation can be improved is with broad federal privacy legislation effectively updating the ECPA of 1986 to the technological advances and internet landscape of 2018.

[79] James J. Choi, David Laibson, Brigitte Madrian, Andrew Metrick, *For Better or For Worse: Default Effects and 401(k) Savings Behavior, in* PERSPECTIVES ON THE ECONOMICS OF AGING, David Wise (Ed.). University of Chicago Press, Chicago, IL, 81 (2004).