2015

Against Jawboning

Derek E. Bambauer

Article

Against Jawboning

Derek E. Bambauer[†]

If you aren't a good rabbit and don't start eating the carrot, I'm afraid we're all going to be throwing the stick at you.

-Representative James Sensenbrenner, pressing U.S. Internet Service Provider Association to adopt putatively volun-

tary data retention scheme.[1]

INTRODUCTION

Many people love Google, but nobody roots for Goliath.[2]

Google's gains made Goliath a target for jawboning. In 2014, Google was experiencing newfound success in its nascent efforts in American politics. The company's support for network neutrality aligned it with other tech firms, helping influence the Federal Communications Commission (FCC) to adopt open Internet rules.[3] It headed off an antitrust investigation into the company's algorithm for ranking its search results.[4] Perhaps most importantly, in 2011–2012, Google helped lead the fight to defeat a pair of federal bills favored by content providers, the Stop Online Piracy Act (SOPA) and PROTECT IP Act, that

---

† Professor of Law, University of Arizona James E. Rogers College of Law. I owe thanks for helpful suggestions and discussion to Jack Balkin, Jane Bambauer, Ian Bartrum, Andy Coan, Aliza Cover, Sarah Haan, Dan Hunter, Margaret Kwoka, Saul Levmore, Fred von Lohmann, Dave Marcus, Michael Montgomery Mason, Toni Massaro, Thinh Nguyen, Carolina Nuñez, Michael Risch, Shaakirrah Sanders, Michalyn Steele, Peter Swire, Alan Trammell, the participants at the Freedom of Expression Scholars Conference at Yale Law School, and the participants at the Rocky Mountain Junior Scholars Forum 2014. Thanks go to Maureen Garmon for expert research assistance. I welcome comments at <derekbambauer@email.arizona.edu>.

1. *See* Declan McCullagh, *DOJ Pressed for Details on Internet Tracking Plan*, CNET NEWS (Jan. 25, 2011), http://www.cnet.com/news/doj-pressed-for-details-on-internet-tracking-plan.

2. Wilt Chamberlain, the legendary National Basketball Association player, complained that "Nobody roots for Goliath." Larry Schwartz, *Wilt Battled "Loser" Label*, ESPN, https://espn.go.com/sportscentury/features/00014133.html (last visited Oct. 13, 2015).

3. *See* Bill Chappell, *FCC Approves Net Neutrality Rules for "Open Internet,"* NPR (Feb. 26, 2015), http://www.npr.org/blogs/thetwo-way/2015/02/26/389259382/net-neutrality-up-for-vote-today-by-fcc-board; Brian Fung, *Google, Netflix Lead Nearly 150 Tech Companies in Protest of FCC Net Neutrality Plan*, WASH. POST (May 7, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/07/google-netflix-lead-nearly-150-tech-companies-in-protest-of-fcc-net-neutrality-plan; Brian Fung, *Google's Studied Silence on Net Neutrality Has Finally Broken*, WASH. POST (Sept. 10, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/10/googles-studied-silence-on-net-neutrality-has-finally-broken; Tom Wheeler, *FCC Chairman Tom Wheeler: This Is How We Will Ensure Net Neutrality*, WIRED (Feb. 4, 2015), http://www.wired.com/2015/02/fcc-chairman-wheeler-net-neutrality.

4. *See* Craig Timberg, *FTC: Google Did Not Break Antitrust Law with Search Practices*, WASH. POST (Jan. 3, 2013), http://www.washingtonpost.com/business/technology/ftc-to-announce-google-settlement-today/2013/01/03/ecb599f0-55c6-11e2-bf3e-76c0a789346f_story.html.

threatened Internet firms with liability if they failed to undertake new copyright enforcement measures.[5]

In the struggle between Hollywood and Silicon Valley, Google won.[6] Along with the Obama Administration and an ad hoc coalition of Internet users and interest groups, the firm forced the abandonment of the bills.[7] Internet firms had displayed a new seriousness about flexing political muscle,[8] and Hollywood, accustomed to having its way with intellectual property policy, reeled in defeat.[9]

But SOPA was not dead—merely driven underground. Content companies quietly regrouped. Rebuffed at the federal level, the firms, led by the movie studios' lobbying arm, the Motion Picture Association of America (MPAA), turned their attention to state regulators. In particular, the MPAA sought assistance from state attorneys general. Hollywood succeeded: by November 2013, the National Association of Attorneys General was holding a special meeting about pressuring Google to deal with copyright infringement—a meeting attended by the MPAA's outside counsel Thomas Perrelli, of the prominent law firm Jenner & Block.[10] In December 2013, Connecticut's Attor-

---

5. *See* PROTECT IP Act of 2011, S. 968, 112th Cong. (2011), http://www.leahy.senate.gov/imo/media/doc/BillText-PROTECTIPAct.pdf; Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011), https://www.congress.gov/bill/112th-congress/house-bill/3261/text; Mark Lemley et al., *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34, 34 (2011); Dan Mitchell, *The Secret Behind the SOPA Defeat*, FORTUNE (Jan. 31, 2012), http://fortune.com/2012/01/31/the-secret-behind-the-sopa-defeat.

6. *See* Michael Crowley, *Washington SOPA Opera: Lobbying Power Shifts from Hollywood to Silicon Valley*, TIME (Jan. 20, 2012), http://swampland.time.com/2012/01/20/washington-sopa-opera-lobbying-power-shifts-from-hollywood-to-silicon-valley.

7. *See* Victoria Espinel et al., *Combating Online Piracy While Protecting an Open and Innovative Internet*, WE THE PEOPLE (Jan. 13, 2012), https://petitions.whitehouse.gov/response/combating-online-piracy-while-protecting-open-and-innovative-internet; Mitchell, *supra* note 5.

8. *See* Crowley, *supra* note 6; Jennifer Martinez et al., *SOPA's Surprise Hollywood Ending*, POLITICO (Jan. 20, 2012), http://www.politico.com/story/2012/01/sopas-surprise-hollywood-ending-071746; Mitchell, *supra* note 5.

9. *See* Crowley, *supra* note 6; Pamela McClintock, *MPAA Chief Christopher Dodd Says SOPA Debate Isn't over, Defends Hosting Harvey Weinstein Even as He Attacked over "Bully,"* HOLLYWOOD REP. (Apr. 5, 2012), http://www.hollywoodreporter.com/news/mpaa-christopher-dodd-sopa-bully-harvey-weinstein-ratings-308359.

10. *See* Russell Brandom, *Project Goliath: Inside Hollywood's Secret War Against Google*, VERGE (Dec. 12, 2014), http://www.theverge.com/2014/12/12/7382287/project-goliath; Joe Mullin, *Hollywood v. Goliath: Inside the Aggressive Studio Effort To Bring Google To Heel*, ARS TECHNICA (Dec. 19, 2014), http://arstechnica.com/tech-policy/2014/12/how-hollywood-spurned-by-congress-pressures-states-to-attack-google.

ney General contacted the MPAA for a list of things to demand in a meeting with the search engine's executives.[11] And in January 2014, thirteen state attorneys general met with Google General Counsel Kent Walker regarding search results that list infringing content.[12]

The MPAA found two especially willing collaborators in Mississippi Attorney General Jim Hood and Nebraska Attorney General Jon Bruning. Before the January 2014 meeting, Perrelli noted in an e-mail that Hood "wants Google to delist pirate sites."[13] And in February 2014, Bruning—to whom both the MPAA and movie studios made campaign donations the following month[14]—discussed using civil subpoenas, lawsuits, and media outreach "to alert consumers to Google's 'bad acts.'"[15] Shortly thereafter, Perrelli described plans to have his firm draft civil subpoenas that Bruning and Hood could use, and suggested that "[s]ome subset of AGs (3–5, but Hood alone if necessary) should move toward issuing CIDs [Civil Investigative Demands] before mid-May."[16] Here, for the first time, the MPAA assigned Google its code name: Goliath.[17] Later that year, Jenner & Block drafted, and Hood signed, a subpoena to Google about videos promoting steroid and other drug use, depicting pornography, and infringing copyright. In December 2014, Google filed suit in federal court in Mississippi to block Hood's investigation,[18] as e-mail messages and other documents from Project Goliath were brought to light by the hack of Sony Pictures' computer systems.[19]

This Article focuses not on the problems with Hood's subpoena, but with the events that led up to it. Once Hood followed through on his threats with formal legal process, Google could

---

11. *See* Mullin, *supra* note 10.

12. *See id.*

13. *Id.*

14. *See* Nick Wingfield & Eric Lipton, *Google's Detractors Take Their Fight to the States*, N.Y. TIMES (Dec. 16, 2014), http://www.nytimes.com/2014/12/17/technology/googles-critics-enlist-state-attorneys-general-in-their-fight.html?ref=technology&_r=0.

15. Mullin, *supra* note 10 (quoting Bruning).

16. *Id.* (quoting Perrelli e-mail).

17. *See id.*; Brandom, *supra* note 10 (quoting Perrelli e-mail).

18. *See* Memorandum of Law in Support of Plaintiff Google Inc.'s Motion for Temporary Restraining Order and Preliminary Injunction, Google Inc. v. Hood, No. 3:14-cv-981-HTW-LRA (N.D. Miss. Dec. 19, 2014) [hereinafter Memorandum of Law].

19. *See* Brandom, *supra* note 10; Andrea Peterson, *The Sony Pictures Hack, Explained*, WASH. POST (Dec. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained.

challenge it in court (successfully, as it turns out).[20] Prior to that, Hood and the other attorneys general were jawboning the search engine—they sought to coerce the company based on threatened action at the edges of or wholly outside their legal authority. The difficulty with the efforts by Hood and his counterparts is not simply the motivation; state officials advocate for interest groups constantly. The issue is that Hood threatened Google despite lacking authority over the subject matter of his investigation. Regulation of drugs such as steroids and their advertising is governed by federal law,[21] and states may enforce those provisions in only a small number of circumstances.[22] Under the Communications Decency Act (CDA), Google enjoys immunity from state criminal prosecution or civil liability based on third-party content, such as the drug advertising or pornography to which Hood objected.[23] In addition, Google enjoys immunity from copyright liability for hosting,[24] caching,[25] or linking to infringing material,[26] so long as it takes a statutorily-prescribed set of precautions. From a legal perspective, Hood's threats were bluffs: he did not have the power to compel Google to adhere to his demands.

So why would Hood or other attorneys general bluff, and why might Google obey? There are two reasons: cost and uncertainty. As to cost, even a subpoena that was ultra vires—beyond the official's power—would cause Google to incur poten-

---

20. *See* Memorandum of Law, *supra* note 18; Russell Brandom, *Google Gets an Early Win in Fight Against Mississippi Attorney General's Subpoena*, VERGE (Mar. 2, 2015), http://www.theverge.com/2015/3/2/8135205/google-jim-hood-goliath-subpoena-case-injunction (describing preliminary injunction barring Hood's investigation).

21. *See* 21 U.S.C. § 337(a) (2006).

22. *See* 21 U.S.C. § 337(b) (allowing states to bring claims for mislabeling). The Food and Drug Administration contends that pre-emption of state drug advertising regulation is complete and unequivocal. *Requirements on Content and Format of Labeling for Human Prescription Drug and Biological Products*, 71 FED. REG. 3922, 3934 (Jan. 24, 2006) ("FDA believes that under existing preemption principles, FDA approval of labeling under the act . . . preempts conflicting or contrary State law.").

23. *See* 47 U.S.C. § 230(c)(1) (2006) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."); 47 U.S.C. § 230(e)(3) ("No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."); Backpage.com v. Cooper, 939 F. Supp. 2d 805, 822 (M.D. Tenn. 2013); GoDaddy.com v. Toups, 429 S.W.3d 752, 758 (Tex. App. 2014).

24. *See* 17 U.S.C. § 512(c) (2012).

25. *See* 17 U.S.C. § 512(b).

26. *See* 17 U.S.C. § 512(d).

tially significant expense.[27] Lawyers at WilmerHale—Google's outside counsel—do not come cheap, and if Hood defeated the motion for the temporary restraining order, Google would have had to comply with burdensome discovery.[28] And the potential costs were more than pecuniary—the MPAA planned to allocate budget to media outreach efforts designed to harm Google's reputation.[29] Even false accusations can wound.

And, the outcome was not certain: courts differ on statutory interpretation, and can make mistakes. For example, appellate courts interpret the scope of immunity under the CDA differently.[30] Contrary to federal and state rules of civil procedure, judges not infrequently seek to bind Google to decisions where it is not a party.[31] Jawboning transfers much of the risk of enforcement to the target. Enforcement may be a lottery ticket for the regulator threatening action, but the potential windfall may be enough to shape the regulated party's conduct.[32] Thus,

---

27. *See* Nathan A. Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1522 (2013) (discussing cost deterrence).

28. *See* Memorandum of Law, *supra* note 18, at 33, 36 (describing subpoena as "unreasonable, retaliatory, and burdensome" and listing Google's counsel from WilmerHale).

29. *See* Mullin, *supra* note 10 (quoting e-mail from MPAA counsel Fabrizio discussing budget to be spent on "seed media stories based on investigation and AG actions").

30. *Compare* Perfect 10, Inc. v. CCBill L.L.C., 488 F.3d 1102, 1118–19 (9th Cir. 2007) (immunizing payment provider and Web host against claimed infringements of state rights of publicity based on 47 U.S.C. § 230), *with* Universal Commc'ns Sys., Inc. v. Lycos, Inc. 478 F.3d 413, 442–43 (1st Cir. 2007) (stating that a claim under state-based trademark law would not be subject to Section 230 immunity).

31. *See* Memorandum and Order, Arista Records v. Vita Tkach, No. 1:15-cv-03701 (S.D.N.Y. June 3, 2015), http://www2.bloomberglaw.com/public/desktop/document/Arista_Records_LLC_et_al_v_Vita_Tkach_et_al_Docket_No_115cv03701_/3 (holding domain name service provider subject to injunction against online file sharing service Grooveshark because Court concluded provider was in active concert with Grooveshark); Order Denying on Reconsideration Plaintiffs' Motion to Hold Public Interest Registry in Contempt of this Court's December 2, 2010, and December 20, 2010, Orders, North Face Apparel Corp. v. Fujian Sharing Imp. & Exp. Ltd., No. 1:10-cv-01630-AKH (S.D.N.Y. June 24, 2011), http://www.scribd.com/doc/58810497/North-Face-v-Fujian-Sharing-10-CV-1630-S-D-N-Y-6-24-11 (holding non-party domain name registrar could be bound by injunction against counterfeiting defendant because registrar aided and abetted defendant by resolving its domain names); Eric Goldman, *A New Way To Bypass 47 USC 230? Default Injunctions and FRCP 65*, TECH. & MKTG. L. BLOG (Nov. 10, 2009), http://blog.ericgoldman.org/archives/2009/11/a_new_way_to_by.htm. *But see* Blockowicz v. Williams, 630 F.3d 563, 569 (7th Cir. 2010) (confirming non-party Web host could not be compelled to remove material). I thank Fred von Lohmann for referring me to the *North Face* case.

32. *Cf.* GUIDO CALABRESI, THE COSTS OF ACCIDENTS 91–92 (Yale Univ.,

uncertainty creates expected cost for the target in addition to the transaction costs described above. Jawboning can be effective even when operating at the limits of a government official's powers.

The term "jawboning" is Biblical in origin: Samson killed a thousand men using a seemingly weak tool—a donkey's jawbone.[33] Legal scholarship borrowed the concept first to denote informal pressures by Presidents[34] and agency heads[35] on recalcitrant bureaucracies, and more recently to stand for suasion through informal contacts by regulators generally,[36] including members of Congress.[37] This Article employs the term to connote a specific type of informal pressure by a government actor on a private entity: one that operates at the limit of, or outside, that actor's authority.[38] This Article then assesses jawboning in one particular context—regulation of Internet intermediaries and the information they disseminate. The Internet provides a useful context for studying jawboning, because the larger libertarian trend in regulation of the Net leads would-be regulators to employ informal rather than formal means.[39] This Article argues that like Samson, state regulators wielding seemingly ineffectual weapons—informal enforcement based on murky au-

---

1970) (describing how uncertainty in accident incidence impedes optimal allocation of costs).

33. *Judges* 15:15 (New Am. Ed.) ("Near him was the fresh jawbone of an ass; he reached out, grasped it, and with it killed a thousand men.").

34. *See* Paul R. Verkuil, *Jawboning Administrative Agencies: Ex Parte Contacts by the White House*, 80 COLUM. L. REV. 943, 943 (1980).

35. *See* Symposium, *The Legacy of Justice Arthur Goldberg*, 29 J. MARSHALL J. COMPUTER & INFO. L. 285, 301 (2012) (describing Goldberg's "suggest[ion] that the [Kennedy] administration implement 'wage and price' guidelines based on what's called jawboning").

36. *See* Jean Braucher, *Humpty Dumpty and the Foreclosure Crisis: Lessons from the Lackluster First Year of the Home Affordable Modification Program (HAMP)*, 52 ARIZ. L. REV. 727, 753–54 (2010); L.A. Powe, Jr., *Red Lion and Pacifica: Are They Relics?*, 36 PEPP. L. REV. 445, 461–62 (2009); David Zaring, *Administration by Treasury*, 95 MINN. L. REV. 187, 209–10 (2010).

37. *See* Jeffrey A. Love & Arpit K. Garg, *Presidential Inaction and the Separation of Powers*, 112 MICH. L. REV. 1195, 1233 (2014).

38. *See infra* Part II. Firms may also engage in self-regulation in the face of impending governmental regulation, as when the National Advertising Division of the Council of Better Business Bureaus created the Children's Advertising Review Unit (CARU) in 1974 to forestall a Federal Trade Commission proposal to limit ads directed at children. Angela J. Campbell, *Self-Regulation and the Media*, 51 FED. COMM. L.J. 711, 735–36 (1999). I thank Peter Swire for this example.

39. *See* Annemarie Bridy, *Internet Payment Blockades*, FLA. L. REV. (forthcoming 2015) (manuscript at 1), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=24940 19.

thority—appear outgunned; yet like Samson, they achieve surprisingly-effective results once the contest begins.

This approach places the Article at the intersection of three contentious scholarly debates. The first focuses on how government ought to respond to disfavored speech—whether via targeted counterspeech,[40] tolerant pluralism,[41] promotion of responsibility as a means towards self-government,[42] or legal prohibition.[43] The second probes the limits of government's authority to regulate expression[44] and whether some disfavored content may be subject to controls because it is not "speech" under the First Amendment.[45] This debate has recently become bound up in Internet-related questions, such as those about search engines,[46] algorithmically-generated information,[47] and the role of technology in authorship.[48] Some scholars defend informal enforcement as more efficient and cost-effective, desirable for industries undergoing dynamic change, and more readi-

40. *See* COREY BRETTSCHNEIDER, WHEN THE STATE SPEAKS, WHAT SHOULD IT SAY? 80–104 (Princeton Univ. Press, 2012). *But see* Frank I. Michelman, *Legitimacy and Autonomy: Values of the Speaking State*, 79 BROOK. L. REV. 985, 985–1004 (2014); Robin West, *Liberty, Equality, and State Responsibilities*, 79 BROOK. L. REV. 1031, 1031–45 (2014).

41. *See* John D. Inazu, *A Confident Pluralism*, 88 S. CAL. L. REV. 587 (2015).

42. *See* JAMES E. FLEMING & LINDA C. MCCLAIN, ORDERED LIBERTY 38–39, 115–24 (Harv. Univ. Press, 2013). *But see* Robin West, *Sovereign Citizens and Civic Responsibility*, CONCURRING OPINIONS (Mar. 1, 2013), http://concurringopinions.com/archives/2013/03/sovereign-citizens-and-civic-responsibility.html.

43. *See* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 142 (Harv. Univ. Press, 2014); Mary Anne Franks, *Sexual Harassment 2.0*, 71 MD. L. REV. 655, 657 (2012).

44. *See, e.g.*, Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 58 (2014).

45. *See id.* at 62. *See generally* Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 NW. U. L. REV. 105, 117–24 (2010); Daniel J. Solove & Neil M. Richards, *Rethinking Free Speech and Civil Liability*, 109 COLUM. L. REV. 1650, 1652 (2009).

46. *See generally* Oren Bracha, *The Folklore of Informationalism: The Case of Search Engine Speech*, 82 FORDHAM L. REV. 1629 (2014); James Grimmelmann, *Speech Engines*, 98 MINN. L. REV. 868 (2014); Tim Wu, *Machine Speech*, 161 U. PA. L. REV. 1495, 1496–98 (2013).

47. *See generally* Derek E. Bambauer, *Copyright = Speech*, 65 EMORY L.J. (forthcoming 2015); Annemarie Bridy, *Coding Creativity: Copyright and the Artificially Intelligent Author*, 5 STAN. TECH. L. REV. 1 (2012).

48. *Compare* Derek E. Bambauer, *Exposed*, 98 MINN. L. REV. 2025, 2070–78 (2014) (arguing that copyright law should evolve to recognize multiple authors), *with* Rebecca Tushnet, *How Many Wrongs Make a Copyright?*, 98 MINN. L. REV. 2346, 2348 (2014) (disagreeing with the argument that the definition of authorship should change).

ly adapted to new circumstances than formal measures.[49] But they are the minority. Most scholars decry informal enforcement,[50] calling it an approach that is unfair,[51] contrary to notions of limited government,[52] and likely to impose unduly onerous regulatory burdens.[53]

This Article brings these debates into fruitful dialogue with one another and injects useful notes into each of them. For the first debate, it aligns government responses along a continuum of coercion, arguing that more coercive responses must be channeled into formal legal mechanisms to obtain legitimacy. For the second, it elucidates the problems with informal enforcement of policies about expression, which readily evades constitutional and statutory constraint. And for the third, it assesses informal pressures in a provocative context—the regulation of speech on Internet platforms—to suggest that legitimacy varies not with industry or cost, but with deeper structural commitments to constraining government.

This Article contends that, regardless of whether jawboning is suspect generally, it is pernicious when applied to Internet intermediaries regarding the content that they provide. Internet platforms such as Google, Twitter, Facebook, and

---

49. *See* Jacob E. Gersen, *Legislative Rules Revisited*, 74 U. CHI. L. REV. 1705, 1720–22 (2007) (arguing that the fear that informal agency rulemaking avoids scrutiny is unfounded, because informal rules are subject to serious judicial scrutiny *ex post*); Jacob E. Gersen & Eric A. Posner, *Soft Law: Lessons from Congressional Practice*, 61 STAN. L. REV. 573, 626 (2008) (contending that informal enforcement is "not a second-best, but is simply an alternative regulatory instrument that has advantages that formal legislation lacks"); Tim Wu, *Agency Threats*, 60 DUKE L.J. 1841, 1848 (2011) (arguing that informal enforcement is well-suited to dynamically changing industries); David Zaring, *Best Practices*, 81 N.Y.U. L. REV. 294, 298 (2006) (arguing that "best practices" rulemaking, by which an agency leads not by hard rules but by example, can be efficient and effective).

50. *See* Jerry Brito, *"Agency Threats" and the Rule of Law: An Offer You Can't Refus*e, 37 HARV. J.L. & PUB. POL'Y 553, 554 (2014); Brent Skorup & Adam Thierer, *Uncreative Destruction: The Misguided War on Vertical Integration in the Information Economy*, 65 FED. COMM. L.J. 157, 196–97 (2013); *see also* Wu, *supra* note 49 (admitting that "[t]he scholarly presumption is that rulemaking or formal adjudication is an intrinsically superior process for most agency action.").

51. *See* Thomas O. McGarity, *Some Thoughts on "Deossifying" the Rulemaking Process*, 41 DUKE L.J. 1385, 1396 (1992).

52. *See* Robert A. Anthony, *Interpretive Rules, Policy Statements, Guidances, Manuals, and the Like—Should Federal Agencies Use Them To Bind the Public?*, 41 DUKE L.J. 1311, 1312 (1992).

53. *See* Lars Noah, *Administrative Arm-Twisting in the Shadow of Congressional Delegations of Authority*, 1997 WIS. L. REV. 873, 875 (1997).

Instagram are the new gatekeepers for online content.[54] Indeed, the story of the modern commercial Internet is largely one about intermediaries.[55] Material de-listed from Google's search results or deleted from a Twitter feed simply disappears for practical purposes.[56] Jawboning that targets platforms over information they carry is normatively illegitimate for three principal reasons. First, platforms are structurally vulnerable to informal pressures. They lack robust incentives to protect third-party content and instead are likely to cave under pressure.[57] Second, the First Amendment institutionalizes a strong preference, if not a command, for government actors to channel regulatory demands via formal mechanisms rather than informal ones.[58] This is because speech is at once strong and weak: strong in its power to change minds and policies and weak because it is readily suppressed, even in the low-cost ecosystem of the Internet.[59] Information online is an attractive target and one that may be poorly defended. Lastly, from the perspective of a process-based approach to decisions about content, jawboning is less legitimate than actions taken through formal chan-

54. I use "intermediary" and "platform" interchangeably, for the sake of variety. I define the terms as denoting Internet entities that enable communication by others. This is similar to how experts such as Marc Andreessen define it, but my view of "programmability" is broader: protocols such as SMTP and TCP/IP are APIs in that they enable programmatic interaction, so entities such as Internet Service Providers would fall within my definition of "platform." *See* Marc Andreessen, *The Three Kinds of Platforms You Meet on the Internet*, PMARCA BLOG (Sept. 16, 2007), http://blog.pmarca.com/2007/09/the-three-kinds.html. *But see* Tarleton L. Gillespie, *The Politics of Platforms*, 12 NEW MEDIA & SOC'Y 347, 348 (2010) (discussing "the discursive work that prominent digital intermediaries, especially YouTube, are undertaking, by focusing on one particular term: 'platform'").

55. *See* Derek E. Bambauer, *Middlemen*, 64 FLA. L. REV. F. 64, 64 (2013) (discussing the dominant role of Internet intermediaries). *See generally* Douglas Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221 (2006); Jacqueline D. Lipton, *Law of the Intermediated Information Exchange*, 64 FLA. L. REV. 1337 (2012); Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239 (2005).

56. *See* Jeffrey Rosen, *The Delete Squad*, NEW REPUBLIC (Apr. 29, 2013), http://www.newrepublic.com/article/113045/free-speech-internet-silicon-valley-making-rules.

57. *See* Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 28–32 (2006).

58. *See* Derek E. Bambauer, *Orwell's Armchair*, 79 U. CHI. L. REV. 863, 899–905 (2012) [hereinafter Bambauer, *Orwell's Armchair*]; Philip Hamburger, *Unconstitutional Conditions: The Irrelevance of Consent*, 98 VA. L. REV. 479, 489, 492–504 (2012).

59. *See* Hamburger, *supra* note 58, at 492–93; Kreimer, *supra* note 57.

nels, which are more likely to be transparent and accountable.

This Article has three more Parts. Part I describes the rise of jawboning as a concept and offers a series of case studies, showing that American government actors increasingly deploy the practice. Part II evaluates the legitimacy of jawboning, and concludes that the tactic is normatively inferior to formal modes of state action. Part III considers possible responses to the increase of illegitimate informal enforcement. This Article concludes by exploring how the jawboning analysis can be applied beyond Internet speech and how it can offer guidance in new regulatory contexts.

I. THE RISE OF JAWBONING

This Part argues that jawboning—enforcement through informal channels, where the underlying authority is in doubt—is on the rise, driven by a libertarian trend in Internet regulation that constrains more formal actions. It then offers four additional, recent case studies—Backpage, data retention, Six Strikes, and network neutrality—as evidence of the increasingly widespread deployment of jawboning.

A. THE NET'S LIBERTARIAN TREND

The rise in jawboning is a counterpoint to, and partly a consequence of, the deregulatory trend regarding online platforms and their content. This libertarian evolution appears puzzling, for there is a wide range of Internet material that is routinely decried: private information about individuals' finances,[60] sex habits,[61] or buying patterns[62]; pornography and other indecent material;[63] hate speech;[64] copyright infringe-

60. *See, e.g.*, Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. (forthcoming 2015) (manuscript at 23–24); Paul Ziobro & Danny Yardon, *Target Now Says 70 Million People Hit in Data Breach*, WALL ST. J. (Jan. 10, 2014), http://www.wsj.com/articles/SB10001424052702303754404579312232546392464.

61. *See generally* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345 (2014); Ryan Singel, *Security Researcher Wants Lube Maker Fined for Privacy Slip*, WIRED (July 10, 2007), http://www.wired.com/2007/07/security-resear.

62. *See, e.g.*, David Lazarus, *Verizon's Super-Cookies Are a Super Privacy Violation*, L.A. TIMES (Feb. 2, 2015), http://www.latimes.com/business/la-fi-lazarus-20150203-column.html.

63. *See generally* Cheryl B. Preston, *Making Family-Friendly Internet a Reality: The Internet Community Ports Act*, 2007 BYU L. REV. 1471 (2007).

64. *See* Danielle Keats Citron, *Civil Rights in Our Information Age*, *in* THE OFFENSIVE INTERNET 31 (Saul Levmore & Martha C. Nussbaum eds., 2010); Alexander Tsesis, *Hate in Cyberspace: Regulating Hate Speech on the*

ment;[65] pro-drug use information;[66] content encouraging eating disorders;[67] information advocating suicide;[68] ads for prostitution;[69] and so forth. Each issue has groups that press strongly for greater controls over information, particularly controls that target platforms.

Yet, in the United States, the trend is clearly towards forbearance rather than oversight. The history of attempted regulation is one of frequent failure. The Supreme Court struck down two federal statutes seeking to safeguard minors from indecent online material on constitutional grounds,[70] and lower federal courts followed their example by invalidating similar state laws.[71] Two proposed bills that would have counteracted sites that enable intellectual property infringement by cutting off their financial support, forcing their removal of search results, and blocking domain name services faltered in the wake of popular discontent and tech industry opposition.[72] Data retention proposals, a hardy Congressional perennial, have failed to make any significant progress.[73] And the long-running law enforcement effort to limit encryption of material has been stymied to date.[74]

Internet, 38 SAN DIEGO L. REV. 817 (2001).

65. *See, e.g.*, McClintock, *supra* note 9.

66. *See* Douglas A. Berman, *Previewing the Advocacy Battle in Florida over 2014 Medical Marijuana Initiative*, MARIJUANA L. POL'Y & REFORM (Aug. 18, 2014), http://lawprofessors.typepad.com/marijuana_law/2014/08/previewing-the-advocacy-battle-in-florida-over-2014-medical-marijuana-initiative.html; Elizabeth Nolan Brown, *State Attorneys General to Google: Censor or Be Censored*, REASON (Apr. 17, 2014), http://reason.com/blog/2014/04/17/google-censored-state-attorneys-general.

67. *See, e.g.*, Mark L. Norris et al., *Ana and the Internet: A Review of Pro-Anorexia Websites*, 39 INT'L J. EATING DISORDERS 443 (2006); Jennifer Van Pelt, *Eating Disorders on the Web—The Pro-Ana/Pro-Mia Movement*, 9 SOC. WORK TODAY 20 (Sept./Oct. 2009), http://www.socialworktoday.com/archive/092109p20.shtml.

68. *See* Lucy Biddle et al., *Suicide and the Internet*, 336 BMJ 800 (2008).

69. *See* Nicholas D. Kristof, *Where Pimps Peddle Their Goods*, N.Y. TIMES, Mar. 18, 2012, at SR1.

70. Ashcroft v. Am. Civil Liberties Union, 535 U.S. 564, 586 (2002) (enjoining governmental enforcement of the Child Online Protection Act); Reno v. Am. Civil Liberties Union, 521 U.S. 844, 882 (1997) (holding that sections 223(a) and 223(d) of the Communications Decency Act abridge the First Amendment's free speech protection).

71. *See* Bambauer, *Orwell's Armchair*, *supra* note 58, at 878–79.

72. *See supra* note 5.

73. *See infra* Part I.C.

74. *See* Herb Lin, *Echoes from the Past on Encryption*, LAWFARE (Feb. 18, 2015), http://www.lawfareblog.com/2015/02/echoes-from-the-past-on-encryption (noting that despite two decades of debate, the government has taken no steps to limit encryption).

In addition to content control efforts that have failed in Congress or the courts, successful legislation and doctrinal developments have tended to protect platforms against liability. Section 230 of the CDA immunizes interactive computer services against most state tort and criminal law.[75] Title II of the Digital Millennium Copyright Act (DMCA) provides a safe harbor from copyright liability for service providers who implement a fairly minimal set of precautionary measures.[76] Similarly, pre-DMCA copyright precedent tended to impose liability only where platforms had specific knowledge of infringing material on their systems, or where they controlled and monetized that content.[77] Fair use and contract precedent has also been generous to platforms, to the point of rewriting offline case law to accommodate search engines and other intermediaries.[78] In trademark law, circuit courts have immunized platforms such as eBay so long as they follow DMCA-like precautions,[79] and a seminal secondary liability case declined to fault a registrar that registered domain names it knew were infringing.[80] In patent, the Supreme Court interpreted inducement of infringement to exempt a party that performed all but one step of a method patent, even where that party arguably encouraged its customers to take the final step.[81] Tort claims against platforms

---

75. 47 U.S.C. § 230 (2012).

76. 17 U.S.C. § 512 (2012).

77. *See, e.g.*, CoStar Grp. v. LoopNet, Inc., 373 F.3d 544, 556 (4th Cir. 2004) (holding provider not liable for infringing material because it had no knowledge or control of that material); Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., 907 F. Supp. 1361, 1373–77 (N.D. Cal. 1995) (holding that provider could not contribute to infringement without knowledge of or participation in the infringement, and dismissing theory of provider's "vicarious liability").

78. *See* Kelly v. Arriba Soft Corp., 336 F.3d 811, 318–19 (9th Cir. 2003); Field v. Google, Inc., 412 F. Supp. 2d 1106, 1115–16 (D. Nev. 2006). In *Field*, the court found that the plaintiff-author had granted Google an implied license by dint of his failure to use HTML tags to indicate he did not want the search engine to catalog his site. Standard copyright doctrine is that one must affirmatively obtain a license from the copyright owner, rather than the owner needing to signal that there is no such permission. *See id.*

79. *See* Tiffany v. eBay, Inc., 600 F.3d 93, 107 (2d Cir. 2010) (holding that eBay's generalized knowledge of trademark infringement on its site was not sufficient to hold it liable for that infringement).

80. Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980, 980 (9th Cir. 1999).

81. *See* Limelight Networks v. Akamai Tech., 134 S. Ct. 2111, 2115 (2014). *See generally* Michael A. Carrier, Limelight v. Akamai*: Limiting Induced Infringement*, WISC. L. REV. ONLINE (2014), http://wisconsinlawreview.org/wp-content/files/Carrier-WLR-Online-Final.pdf (discussing how *Limelight* weakened infringement doctrine).

that suffer data breaches have failed for a variety of doctrinal reasons.[82] First Amendment safeguards prevent plaintiffs from holding search engines responsible for the content or ordering of their results.[83] Finally, even where platforms are liable for third-party material, such as child pornography, they are held to account only when the firms have actual knowledge of an apparent violation.[84]

There are exceptions, of course, particularly where the content is of the platform's creation. Firms could be liable for creating or knowingly distributing obscene material[85] or child pornography.[86] Despite Section 230 of the CDA's protections, platforms are liable in some circuits for violating a person's right of publicity,[87] and in all circuits if the tortious material is of the firm's creation.[88] They can be sanctioned if they obtain information from their users in violation of the Wiretap Act[89] or the Children's Online Privacy Protection Act,[90] or if they disclose it in violation of the Stored Communications Act.[91] And there are sector-specific privacy and data retention requirements in industries such as health care,[92] publicly traded companies,[93] and finance.[94] Overall, though, Internet platforms face

82. *See generally* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 639–40 (7th Cir. 2007); Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 296–311 (2005); Jacob W. Schneider, Note, *Preventing Data Breaches: Alternative Approaches To Deter Negligent Handling of Consumer Data*, 15 B.U. J. SCI. & TECH. L. 279, 286–90 (2009).

83. *See* Zhang v. Baidu.com, Inc., 10 F. Supp. 3d 433, 439–40 (S.D.N.Y. 2014) (holding that the search engine's blockade of certain search results was protected speech under the First Amendment); Search King v. Google, Inc., No. CIV-02-1457-M, 2003 WL 21464568, at *4 (W.D. Okla. May 27, 2003) (holding Google's page ranking system to be protected speech).

84. *See* 18 U.S.C. § 2258A(a)(1) (2012).

85. *See* 18 U.S.C. §§ 1465, 1466, 1466A (2012).

86. *See* 18 U.S.C. §§ 2252, 2252A, 2258A(e).

87. *Compare* Perfect 10, Inc., v. CCBill L.L.C., 488 F.3d 1102, 118–19 (9th Cir. 2007) (holding claims for infringement of state rights of publicity blocked by 47 U.S.C. § 230), *with* Universal Commc'ns Sys., Inc., v. Lycos, Inc., 478 F.3d 413, 418–19 (1st Cir. 2007) (stating that state-based intellectual property claims are not subject to Section 230 immunity).

88. *See* Fair Hous. Council v. Roommates.com, L.L.C., 521 F.3d 1157, 1162 (9th Cir. 2008) (noting that provider immunity under the CDA applies only if the provider took no part in creating the content).

89. 18 U.S.C. § 2511 (2012).

90. 15 U.S.C. §§ 6501–06 (2012); 16 C.F.R. § 312 (2015).

91. 18 U.S.C. § 2702(a) (2012).

92. *See* 45 C.F.R. § 160 (2015) (setting universal standards for health care industry data sharing and retention).

93. *See* 15 U.S.C. § 7262 (2012) (requiring certain publicly-traded companies to report on the "internal control" of their data).

far fewer content regulations than offline analogues such as television stations[95] and newspapers.[96]

Thus, government regulation of content on Internet platforms is at times constitutionally proscribed, at times forbidden by statute, and at times limited to federal enforcement. These limits have caused would-be regulators to shift to informal efforts. In addition to evading legal constraints, informal enforcement has other benefits for government. It reduces regulatory cost: rather than having to pass laws or promulgate rules, state actors can turn directly to implementing their policies. And, bypassing procedural requirements reduces expenditures as well. Informal enforcement also shifts reputational risk to private actors—it cloaks what is in reality state action in the guise of private choice.[97] Thus, government is less likely to be held to account, either directly or through public criticism. In short, constraints upon direct regulation of platforms and content have forced government actors to become creative with enforcement.

To support the claim that jawboning has become increasingly common, this Article offers four case studies, in addition to the one on Operation Goliath that opened the narrative: Backpage, data retention, Six Strikes, and network neutrality.

B. BACKPAGE: THE INTERNET'S SEEDY SIDE

Backpage.com is the Internet version of a newspaper's classified ads section: one can find ads selling used cars, fishing poles, pets—and sex. The site's "adult" section has a category for escorts, among other options, and prostitution ads are ubiquitous. A study by Arizona State University found that almost eighty percent of the ads in the adult section were for prosti-

94. *See* 15 U.S.C. §§ 6801–08 (2012) (establishing customer privacy standards for financial institutions); 16 C.F.R. §§ 314.1–4.5 (2015) (establishing customer privacy standards for all financial institutions over which the Federal Trade Commission has jurisdiction).

95. *Compare* Ashcroft v. Am. Civil Liberties Union, 542 U.S. 656, 670 (2004) (applying strict scrutiny to regulation of Internet content), *with* Turner Broad. Sys., Inc. v. FCC, 520 U.S. 180, 190 (1997) (applying intermediate scrutiny to regulation of cable television content).

96. For example, newspapers can be liable for publishing defamatory material, while Internet platforms cannot. 47 U.S.C. § 230(c) (2012); *see, e.g.*, N.Y. Times Co. v. Sullivan, 376 U.S. 254, 286 (1964) (noting that the defendant-newspaper could have been held liable for libel had the plaintiff shown that the newspaper had acted with "actual malice").

97. *See* Bambauer, *Orwell's Armchair*, *supra* note 58, at 901 (arguing that informal enforcement via persuasion runs the risk that "governmental goals may be disguised as objectives of private firms").

tutes.[98] Moreover, some of those being advertised as available for sex are minors.[99]

Those ads have made Backpage a target. State attorneys general have accused Backpage of being a "hub for illegal services [that] has proven particularly enticing for those seeking to sexually exploit minors."[100] Columnist Nicholas Kristof of the *New York Times* lambasted the site as "a godsend to pimps, allowing customers to order a girl online as if she were a pizza."[101] And Detroit police suggested that the site might be to blame for the murders of women who placed escort service ads on Backpage.[102]

State legislatures in New Jersey, Tennessee, and Washington passed bills targeting Backpage.com.[103] The new laws imposed criminal penalties for knowingly publishing or disseminating commercial sex ads involving minors.[104] Similarly, in 2011, attorneys general from 46 states signed a letter demanding that Backpage substantiate its claims that the site carefully polices ads in the adult section, or face a subpoena.[105]

The problem with the new laws and demands was that they were plainly unenforceable. In 1996, as part of its legislative overhaul of telecommunications regulation, Congress passed (and President Clinton signed) a bill with a provision granting interactive computer services, such as Backpage.com, broad immunity from state civil and criminal claims. Section 230 of the CDA provides that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information

98. J.J. Hensley, *ASU Study: Most Ads on Backpage's Adult Section for Prostitution*, AZCENTRAL (Aug. 25, 2012), http://www.azcentral.com/news/articles/20120824backpage-ads-prostitution-asu.html.

99. *See* Suzanne Choney, *Classified Ad Site Backpage in Crosshairs over Child Sex Ads*, NBC NEWS (July 29, 2013), http://www.nbcnews.com/tech/tech-news/classified-ad-site-backpage-crosshairs-over-child-sex-ads-f6C10789250.

100. Letter from Nat'l Assoc. of Attorneys Gen. to Samuel Fifer, Counsel, Backpage.com (Aug. 31, 2011) [hereinafter N.A.A.G. Letter], http://agportals3bucket.s3.amazonaws.com/uploadedfiles/Home/News/Press_Releases/2011/NAAG_Backpage_Signon_08-31-11_Final.pdf .

101. Nicholas D. Kristof, *How Pimps Use the Web To Sell Girls*, N.Y. TIMES, Jan. 26, 2012, at A31.

102. *See Detroit Police Say Killings May Be Linked to Backpage.com*, KING5 (Dec. 30, 2011), http://www.king5.com/story/local/2015/01/09/13047416.

103. *See* Stephanie Silvano, Note, *Fighting a Losing Battle To Win the War: Can States Combat Domestic Minor Sex Trafficking Despite CDA Preemption?*, 83 FORDHAM L. REV. 375, 390–92 (2014).

104. *Id.*; *see* N.J. STAT. ANN. § 2C:13-10 (2013); TENN. CODE ANN. § 39-13-315 (2014); WASH. REV. CODE ANN. § 9.68A.104 (repealed 2013).

105. N.A.A.G. Letter, *supra* note 100.

content provider."[106] Federal criminal statutes are exempted,[107] but state laws that contravene this provision are expressly blocked from enforcement.[108] A plethora of case law interpreting Section 230 makes clear that statutes like those in New Jersey, Tennessee, and Washington, which sought to hold Backpage liable for content created by its users, were pre-empted.[109] Legal liability under those laws turned upon Backpage's decision to publish or disseminate material created by others, which is precisely the sort of choice protected under Section 230.[110] Furthermore, the legislatures in the three states adopted the new statutes only after years of pressure from their respective law enforcement agencies, and in particular their attorneys general, on Backpage to police its adult section more aggressively.[111] There is no doubt that the firm was the target of the stat-

106. 47 U.S.C. § 230(c)(1) (2012).

107. 47 U.S.C. § 230(e)(1).

108. *See* 47 U.S.C. § 230(e)(3) ("No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.").

109. *See, e.g.*, Universal Commc'ns, Inc. v. Lycos, Inc., 478 F.3d 413, 418–19 (1st Cir. 2007) (finding message board operator protected from liability for content created by user); Carafano v. Metrosplash.com, 339 F.3d 1119, 1125 (9th Cir. 2003) (holding Internet dating site immune from tort liability based on content created by user); Green v. Am. Online (AOL), 318 F.3d 465, 468 (3d Cir. 2003) (immunizing ISP for allegedly failing to police its services for unlawful content created by users). *See generally* David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOYOLA L.A. L. REV. 373 (2010) (performing empirical and doctrinal analysis of Section 230 cases). Tennessee, which sits in the Sixth Circuit, did not have a case from that appellate court interpreting the statute when the legislation passed. *But see* Backpage.com v. Cooper, 939 F. Supp. 2d 805, 822 (M.D. Tenn. 2013) (citing circuit court cases interpreting Section 230's immunity as wide-ranging). Unsurprisingly, however, the Sixth Circuit interpreted Section 230 as every other court of appeals has done once it ruled in 2014. *See* Jones v. Dirty World Entm't Recordings L.L.C., 755 F.3d 398, 413 (6th Cir. 2014).

110. 47 U.S.C. § 230(c)(1). Backpage is clearly an interactive computer service, which the statute defines as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server." 47 U.S.C. § 230(f)(2). Theoretically, a statute could impose liability upon distributors of unlawful content, since the relevant provision addresses only publishers and speakers. However, an early, seminal Fourth Circuit case interpreted distributor liability as a subset of publisher liability, and later courts have adopted that approach. Zeran v. Am. Online, 129 F.3d 327, 332–33 (4th Cir. 1997); *see Jones*, 755 F.3d at 407–08; Barnes v. Yahoo!, 570 F.3d 1096, 1103–05 (9th Cir. 2009); *Green*, 318 F.3d at 470–71.

111. *See* Backpage.com v. Hoffman, No. 13-cv-03952 (DMC)(JAD), 2013 WL 4502097, at *3 (D.N.J. Aug. 20, 2013) (noting New Jersey's statute was expressly modeled on the Washington statute); *Cooper*, 939 F. Supp. 2d at 819 ("Backpage.com has shown sufficient evidence that it is the direct target of the law . . . . Even if the statute did not directly target Backpage.com . . . [it] has

utes.[112] And New Jersey knew its statute was likely unenforceable when the legislation was introduced—by that date, the nearly identical Washington and Tennessee laws had already been blocked by federal district courts in those states.[113] By March 2013, when the New Jersey legislature passed its statute, Washington had agreed not only to work to repeal its law, but to pay Backpage $200,000 in attorneys' fees.[114]

New Jersey, Tennessee, and Washington all responded to the significant problems of prostitution and of sex trafficking in minors through both formal and informal pressures. The states had good reason to try: similar tactics pushed Craigslist to remove its "adult services" section, even though the company had prevailed against attempts to hold it liable under state law.[115] The formal pressures—litigation explicitly targeting Backpage as a hub for illegal sex work—were plainly unlawful. Indeed, the National Association of Attorneys General conceded as much in a 2013 letter urging Congress to amend Section 230—a letter citing Section 230 case law establishing broad immunity that pre-dated the New Jersey, Tennessee, and Washington legislation.[116] This makes the informal pressures used by those states illegitimate as well. Threats to pursue enforcement of the bills unless Backpage complied with demands, such as to monitor and remove content more actively, are not legitimate. Backpage faced unattractive options: comply, risk prosecution

---

nonetheless alleged sufficient facts to establish a credible threat of prosecution . . . ."); Backpage.com v. McKenna, 881 F. Supp. 2d 1262, 1270 (W.D. Wash. 2012) ("Washington legislators have openly stated that the challenged statute is aimed at Backpage.com . . . .").

112. *See Hoffman*, 2013 WL 4502097, at *3; *Cooper*, 939 F. Supp. 2d at 819; *McKenna*, 881 F. Supp. 2d at 1270.

113. *See Hoffman*, 2013 WL 4502097, at *1–2 (noting that the New Jersey legislation was introduced Oct. 4, 2012); *Cooper*, 939 F. Supp. 2d at 816 (noting that the Washington legislation was enjoined preliminarily on July 27, 2012); *id.* at 818 (noting that Tennessee stipulated it would not enforce law during pendency of suit on June 29, 2012).

114. *See Hoffman*, 2013 WL 4502097, at *2 (listing dates); *State Agrees To Work To Repeal Law Opposed by Backpage.com*, Q13 FOX NEWS (Dec. 7, 2012, 8:51 PM), http://q13fox.com/2012/12/07/state-agrees-to-work-to-repeal-law-opposed-by-backpage-com-provide-200k-in-attorneys-fees.

115. *See* M.A. v. Vill. Voice Media Holdings, 809 F. Supp. 2d 1041, 1058–59 (E.D. Mo. 2011); David Sarno, *Craigslist To Remove Erotic Services Section, Monitor Adult Services Posts [Updated]*, L.A. TIMES (May 13, 2009, 8:40 AM), http://latimesblogs.latimes.com/technology/2009/05/craigslist-attorneys-general-erotic-services-prostitution.html.

116. Letter from Nat'l Ass'n of Attorneys Gen. to Senator John Rockefeller IV, Chairman, Senate Comm. on Commerce, Sci., and Transp., et al. (July 23, 2013), https://s3.amazonaws.com/s3.documentcloud.org/documents/739520/ags-anti-230-letter.pdf.

and concomitant damage to the company's business, or undertake the expense of challenging the statutes. The firm chose the third option, and won. But the costs were a waste: it was clear the legislation was pre-empted, and that its reason for passage was to punish Backpage by imposing litigation costs. Government cannot operate outside the law, even for a noble cause—particularly when it attempts to regulate speech.

The states did have lawful options. They could have sought to persuade the Department of Justice to investigate Backpage, since there is a federal criminal statute prohibiting similar conduct featuring minors that is not pre-empted by Section 230.[117] They could have urged consumers to boycott the service if it did not improve its monitoring.[118] They could have expanded law enforcement use of Backpage to prosecute sex traffickers—the site, after all, keeps identifying information and credit card details about advertisers.[119] The states had a range of permissible options, and could have threatened Backpage with any of them if the service failed to comply. Informal enforcement will often be legitimate. Here, though, the absence of any lawful basis for the threats meant that it was not.

C. DATA RETENTION: BUILDING YOUR PERMANENT FILE

The government wants your Internet Service Provider to help it assemble your database of ruin.[120]

---

117. 18 U.S.C. § 1591 (2012); 47 U.S.C. § 230(e)(1) (2012); *see Cooper*, 939 F. Supp. 2d at 825–26 (describing differences between Section 1591 and Tennessee statute).

118. *See, e.g.*, Matt Driscoll, *Mayor McGinn Announces an End to City's Advertising Boycott of Seattle Weekly*, SEATTLE WEEKLY NEWS (Sept. 26, 2012, 12:00 AM), http://www.seattleweekly.com/dailyweekly/2012/09/mayor_mcginn_announces_end_seattles_advertising_boycott_of_seattle_weekly.php (noting that the city ended the boycott after paper owner separated from Backpage).

119. *See* Daniel Fisher, *Backpage Takes Heat, but Prostitution Ads Are Everywhere*, FORBES (Jan. 26, 2012, 9:25 AM), http://www.forbes.com/sites/danielfisher/2012/01/26/backpages-takes-heat-for-prostitution-ads-that-are-everywhere (noting that the person posting the ad highlighted by Nicholas Kristof in the *New York Times* supplied a credit card number that allowed law enforcement to identify him); Eric Nicholson, *Dallas Police Are Now Posting Prostitution Ads on Backpage.com*, DALLAS OBSERVER (Sept. 20, 2013), http://www.dallasobserver.com/news/dallas-police-are-now-posting-prostitution-ads-on-backpagecom-7140623.

120. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1746 (2010) (defining the "database of ruin" as "the worldwide collection of all of the facts held by third parties that can be used to cause privacy-related harm to almost every member of society"). I may be re-interpreting Ohm's concept somewhat; his villains are "identity thieves, blackmailers, and unscrupulous advertisers,"

In April 2005, the Department of Justice pressed ISPs to adopt voluntarily a system of archiving records of users' Internet activities for months, if not years.[121] The Justice Department deployed several arguments. One was reputational: the president of the trade group U.S. Internet Industry Association recounted that, "We were told, 'You're going to have to start thinking about data retention if you don't want people to think you're soft on child porn.'"[122] The government also advanced the specter of mandatory data retention legislation—a proposal that the same administration had rejected a few years earlier as unnecessary and unduly burdensome.[123] The message was clear: keep records voluntarily, or face a potentially costly and cumbersome legal mandate.

Pressure increased in 2006.[124] At the Davos Economic Forum in January, FBI Director Robert Mueller spoke out in favor of harmonizing countries' cybercrime laws to include "standardized regulations and rules relating to data retention."[125] Department of Homeland Security Secretary Michael Chertoff indicated in March 2006 that he too favored such a mandate.[126] ISPs remained reluctant to retain data voluntarily (or to be compelled to do so), citing both the lack of evidence of law enforcement need and potential privacy risks.[127] In April, Attorney General Alberto Gonzales pushed providers during a speech at the National Center for Missing and Exploited Children.[128] After recounting graphic depictions of child pornogra-

---

and regulators his white knights. *Id*. I am perhaps more skeptical of governmental efforts, but regardless of who assembles it, merely having a long-term collection of our Internet activities would pose risks from both public and private actors.

121. Declan McCullagh, *Your ISP as Net Watchdog*, CNET (June 16, 2005, 6:42 AM), http://www.cnet.com/news/Your-isp-as-net-watchdog.

122. *Id.* Even after the attacks of September 11, 2001, the Department of Justice still rejected mandatory data retention. *Id.* at 2 (quoting Mark Richard, Deputy Assistant Attorney Gen., Comments of the United States on the European Commission Communication on Combating Computer Crime at the European Union Forum on Cybercrime at Brussels (Nov. 27, 2001)).

123. *Id.* at 1.

124. *See* Anita L. Allen, *Dredging up the Past: Lifelogging, Memory, and Surveillance*, 75 U. CHI. L. REV. 47, 70 n.86 (2008).

125. Declan McCullagh, *ISP Snooping Gaining Support*, CNET (Apr. 14, 2006, 1:49 PM), http://www.cnet.com/news/isp-snooping-gaining-support.

126. *Id.*

127. *Id.* at 2. Since 1996, law enforcement and other government agencies have the authority to require ISPs to preserve designated records for up to 180 days upon request. Antiterrorism and Effective Death Penalty Act of 1996, 18 U.S.C. § 2703(f) (2012) (effective Apr. 24, 1996).

128. *See* Anne Broache, *U.S. Attorney General Calls for "Reasonable" Data Retention*, CNET (Apr. 20, 2006, 3:58 PM), http://www.cnet.com/news/u-s

phy and sexual abuse, Gonzales stated that "the failure of some Internet service providers to keep records has hampered our ability to conduct investigations in this area," and noted that he had "asked the appropriate experts at the Department to examine this issue and provide [him] with proposed recommendations."[129]

Industry reluctance to adopt data retention, in turn, generated threats from the administration and Congress to seek legislation. Bush administration officials endorsed a congressional proposal for a one-year requirement, and the bill's sponsor in the House of Representatives attacked ISPs for opposing it.[130] Attorney General Gonzales then pressed providers in private meetings to go beyond the proposed legislation and retain identifying records for two years, illustrating his point by sharing pixelated photos of child pornography with network providers.[131]

Jawboning worked, at least in part. At hearings by a House committee on the sexual exploitation of minors, one major ISP, Comcast, agreed to voluntarily retain data for 180 days to aid law enforcement.[132] The Bush administration renewed pressure in 2007, as Representative Lamar Smith introduced a data retention bill, backed by criminal penalties, that would have enabled Attorney General Gonzales to set the scope and requirements for recordkeeping.[133] Even after Gonzales' resignation, the FBI continued to press for the mandate, and proposed expanding its scope to require search engines to maintain records of searches on their sites.[134] The pattern of pressure on ISPs,

---

-attorney-general-calls-for-reasonable-data-retention.

129. Alberto R. Gonzales, Attorney General, Prepared Remarks at the National Center for Missing and Exploited Children (NCMEC) (Apr. 20, 2006), http://www.justice.gov/archive/ag/speeches/2006/ag_speech_060420.html.

130. *See* Anne Broache, *Backer of ISP Snooping Slams Industry*, CNET (May 4, 2006, 9:30 AM), http://www.cnet.com/news/backer-of-isp-snooping-slams-industry; Declan McCullagh, *Republican Politico Endorses Data Retention*, CNET (May 5, 2006, 1:35 PM), http://www.cnet.com/news/republican-politico-endorses-data-retention.

131. *See* Declan McCullagh, *Gonzales Pressures ISPs on Data Retention*, CNET (May 30, 2006, 4:01 PM), http://www.cnet.com/news/gonzales-pressures-ISPs-on-data-retention.

132. *See* Benjamin R. Davis, Comment, *Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance*, 15 J. COMM. L. & POL'Y 119, 157 (2006).

133. *See* Declan McCullagh, *GOP Revives ISP-Tracking Legislation*, CNET (Feb. 7, 2007, 7:07 AM), http://www.cnet.com/news/gop-revives-isp-tracking-legislation.

134. *See* Declan McCullagh, *FBI, Politicos Renew Push for ISP Data Retention Laws*, CNET (Apr. 24, 2008, 6:14 AM), http://www.cnet.com/news/fbi

backed by threats of legislation, continued after the change in control to the Democratic Party under President Obama.[135] Indeed, at a hearing in January 2011, Representative F. James Sensenbrenner Jr., chair of the House Judiciary Subcommittee on Crime, made the threat explicit to the executive director of the U.S. Internet Service Provider Association: "[I]f you aren't a good rabbit and don't start eating the carrot, I am afraid that we are all going to be throwing the stick at you."[136] Whatever the merits of the mixed metaphor, to date the rabbit has spurned the carrot, with no stick forthcoming.

The story of data retention is thus one of an ongoing bluff: administrations of both major political parties cajole ISPs to adopt archiving measures, with the threat (sometimes explicit, sometimes implicit) of costly, onerous legislation if the providers fail to comply. Recording user information has been on the policy agenda of the Department of Justice at least since 1999, when Deputy Attorney General Eric Holder stated that "certain data must be retained by ISPs for reasonable periods of time" to fight child pornography.[137] Under President Obama, the Department of Justice went on record in both 2011 and 2012 to support mandatory data retention legislation.[138] Yet, the closest that Congress has come to enacting legislation was in 2011, when the "Protecting Children From Internet Pornographers Act of 2011" passed the House Judiciary Committee,[139] but failed to progress further.[140] Indeed, in 2006, the Department of

-politicos-renew-push-for-isp-data-retention-laws.

135. *See* Declan McCullagh, *Justice Department Seeks Mandatory Data Retention*, CNET (Jan. 24, 2011, 10:47 PM), http://www.cnet.com/news/justice-department-seeks-mandatory-data-retention.

136. *Data Retention as a Tool for Investigating Internet Child Pornography and Other Crimes: Hearing Before the Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 46 (2011) (statement of Rep. Sensenbrenner, Chairman, Subcomm. on Crime, Terrorism, & Homeland Sec.).

137. Kevin V. Ryan & Mark L. Krotoski, *Caution Advised: Avoid Undermining the Legitimate Needs of Law Enforcement To Solve Crimes Involving the Internet in Amending the Electronic Communications Privacy Act*, 47 U.S.F. L. REV. 291, 341 (2012).

138. *Id.* at 342–43.

139. Protecting Children from Internet Pornographers Act of 2011, H.R. 1981, 112th Cong. (2011), https://www.govtrack.us/congress/bills/112/hr1981 (last visited Oct. 14, 2015).

140. *See* Declan McCullagh, *House Panel Approves Broadened ISP Snooping Bill*, CNET (July 28, 2011, 1:41 PM), http://www.cnet.com/news/house-panel-approves-broadened-isp-snooping-bill.

Justice admitted to reporters in private that the legislation was too controversial to attempt in an election year.[141]

So far, most ISPs have failed to comply, and some have even reduced data retention.[142] Providers resist these pressures for economic reasons. Their customers fear incursions upon privacy and might use the Net less if their activities were recorded. Further, infrastructure costs would rise, perhaps dramatically, if the ISPs were forced into a retention regime.[143] Despite the twin specters of terrorism and child pornography, governments led by both major parties have been utterly unable to pass a data retention bill.[144] Their legal authority to compel preservation remains limited in scope and time: to records identified at the request of a government entity, and to a maximum of 180 days.[145] More systemic data retention requirements could face constitutional challenges as violative of either the First Amendment (by destroying the possibility of anonymous speech) or the Fourth Amendment (by imposing an unconstitutional search).[146] Privacy scholar Catherine Crump notes that the record-keeping requirements have already been approved by the Supreme Court in the Fourth Amendment context, but suggests the First Amendment path has merit.[147]

Thus, efforts to jawbone ISPs into broader archiving not only implicate important First Amendment,[148] Fourth Amendment,[149] and privacy[150] concerns, but also overreach, extending

---

141. *See* Declan McCullagh, *FBI Director Wants ISPs To Track Users*, CNET (Oct. 18, 2006, 6:41 AM), http://www.cnet.com/news/fbi-director-wants-ISPs-to-track-users.

142. *See* Kim Hart, *Yahoo Changes Data-Retention Policy*, WASH. POST (Dec. 17, 2008, 1:50 PM), http://voices.washingtonpost.com/posttech/2008/12/yahoo_changes_data-retention_p.html.

143. *See* Kevin Bohn, *Feds Put Squeeze on Internet Firms*, CNN (May 31, 2006, 9:55 AM), http://www.cnn.com/2006/TECH/internet/05/30/internet.records/index.html; Ellen Nakashima, *Bill Would Make ISPs Keep Data on Users*, WASH. POST (Feb. 13, 2007), https://www.washingtonpost.com/wp-dyn/content/article/2007/02/12/AR2007021201337.html.

144. *See generally* Agatha M. Cole, *Politics, Privacy, and Child Pornography: The Battle over Data Retention and H.R. 1981*, CARDOZO ARTS & ENT. L.J. (Mar. 4, 2012), http://www.cardozoaelj.com/agatha_blog (describing the difficulties of passing data retention legislation).

145. 18 U.S.C. § 2703(f)(2) (2012).

146. *See* Catherine Crump, Note, *Data Retention: Privacy, Anonymity, and Accountability Online*, 56 STAN. L. REV. 191, 196 (2003).

147. *Id.* at 204–05, 223–28.

148. *Cf.* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) (finding right to anonymous political speech protected by First Amendment).

149. *Cf.* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had

beyond any authority the state possesses or could realistically expect to obtain.[151] In the era of pervasive state surveillance of data held by private firms—from Google to Facebook to e-mail providers—government-driven data archiving that operates outside formal legal channels should be viewed as suspect.[152]

D. SIX STRIKES: "THE CAJOLE SET OF ISSUES"

In the summer of 2011, a number of large Internet Service Providers announced that they would increase measures to prevent copyright infringement by their users.[153] The plan, known informally as "six strikes," debuted as a Memorandum of Understanding between the ISPs and content companies such as Walt Disney Studios, Sony Pictures, and Warner Music Group.[154] Providers agreed to process notifications of alleged infringement from the content companies and to impose a series of penalties (euphemistically termed "Copyright Alerts") on the users allegedly engaged in infringement.[155] ISPs agreed to pro-

---

visited in the last week, or month, or year.").

150. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 504–15 (2006) (discussing harms from aggregation and identification of data).

151. *See ECPA (Part I): Lawful Access to Stored Content Before the Subcomm. on Crime, Terrorism, Homeland Sec., & Investigations of the H. Comm. on the Judiciary*, 113th Cong. 63 (2013) (statement of Rep. Sensenbrenner, Chairman, Subcomm. on Crime, Terrorism, Homeland Sec., & Investigations) ("[Passing data retention legislation] is going to be kind of a tough nut to crack.").

152. *See, e.g.*, Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (describing NSA's MUSCULAR program for intercepting internal Google traffic); Glenn Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet*," GUARDIAN (July 31, 2013, 8:56 AM), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (describing NSA tool used to access information such as e-mail content and Facebook chats); Charlie Savage et al., *Hunting for Hackers, N.S.A. Secretly Expands Internet Spying at U.S. Border*, N.Y. TIMES (June 4, 2015), http://www.nytimes.com/2015/06/05/us/hunting-for-hackers-nsa-secretly-expands-internet-spying-at-us-border.html (describing warrantless collection of American data that crosses international borders).

153. MEMORANDUM OF UNDERSTANDING, CTR. FOR COPYRIGHT INFO. 24 (July 6, 2011), http://www.copyrightinformation.org/wp-content/uploads/2013/02/Memorandum-of-Understanding.pdf (listing participating ISPs).

154. *Id.* at 25 (listing participating content owners).

155. *Id.* at 4–14; *see* Annemarie Bridy, *Graduated Response American Style: "Six Strikes" Measured Against Five Norms*, 23 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 1, 5–6 (2012).

vide half the funding for both a system of independent review for challenged notifications[156] and an organization dedicated to implementing the six strikes program.[157]

The ISPs' decision to undertake six strikes is puzzling for at least three reasons. First, providers are almost entirely shielded from liability for transporting or hosting material that infringes copyrights by the safe harbor provisions of the Digital Millennium Copyright Act.[158] Content owners have launched a series of lawsuits against ISPs and Internet platforms over hosting infringing material, without success.[159] Thus, ISPs had little if anything to fear from litigation. Second, the six strikes program risked irritating the ISPs' customers, especially if the harsher mitigation measures contemplated under six strikes were deployed.[160] While consumers generally lack a wide range of choices in broadband service providers, those with more than one option could respond to a Copyright Alert by changing ISPs.[161] Third, Internet providers benefit from infringement.[162]

---

156. MEMORANDUM OF UNDERSTANDING, *supra* note 153, at 14.

157. *Id.* at 4; *see generally* Mary LaFrance, *Graduated Response by Industry Compact: Piercing the Black Box*, 30 CARDOZO ARTS & ENT. L.J. 165 (2012) (describing the formulation of the Memorandum of Understanding and its components).

158. Digital Millennium Copyright Act, 17 U.S.C. § 512 (2012).

159. *See, e.g.*, UMG Recordings v. Shelter Capital Partners L.L.C., 718 F.3d 1006 (9th Cir. 2013); Viacom Int'l v. YouTube, 676 F.3d 19 (2d Cir. 2012); Recording Indus. Ass'n of Am. v. Verizon Internet Servs., 351 F.3d 1229 (D.C. Cir. 2003); *see also* Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1837 (2000). *But see* Complaint for Copyright Infringement, BMG Rights Mgmt. v. Cox Enters., No. 1:14-cv-1611 (LOG/JFA) (E.D. Va. Nov. 26, 2014) (seeking to hold ISP liable for failure to terminate repeat copyright infringers as required under 17 U.S.C. § 512(i)). I thank Fred von Lohmann for pointing me to the pending *Cox* litigation.

160. *See* Annemarie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, 89 OR. L. REV. 81, 101 (2010).

161. FCC, INTERNET ACCESS SERVICES: STATUS AS OF DECEMBER 31, 2013 9 (2014), https://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db1016/DOC-329973A1.pdf (showing over 90% of households are served by two or more ISPs).

162. Some scholars suggest ISPs were willing to adopt six strikes because infringing content was overburdening their networks. *See, e.g.*, Peter K. Yu, *The Graduated Response*, 62 FLA. L. REV. 1373, 1385 (2010) ("ISPs were annoyed by how Internet file-sharers have abused the service by hogging bandwidth, congesting the network, and reducing the overall user experience of most other subscribers."). If this were true, one would expect ISPs independently to take voluntary measures, as Comcast did when it throttled BitTorrent. *See* Comcast v. FCC, 600 F.3d 642, 644 (D.C. Cir. 2010). The fact that ISPs did not do so strongly suggests that this argument for six strikes is incorrect.

Access to costless copyrighted material is attractive to some users, who are willing to pay for faster connections to stream or download the content.[163] Reducing infringement would risk not only driving users away, but also making the ISPs' services less attractive to them. In short, six strikes looked like a bad bargain for ISPs. So why agree to spend money for a program that seemed to offer only costs and not benefits?

The answer is likely jawboning. The Obama administration, via Intellectual Property Enforcement Coordinator Victoria Espinel, was intimately involved in the negotiations between the content companies and the ISPs—on the side of Hollywood.[164] The administration had been interested in forcing ISPs to implement "graduated response" measures—penalizing and eventually disconnecting users who engage in intellectual property infringement—by including such a requirement in the international Anti-Counterfeiting Trade Agreement (ACTA).[165] However, other countries negotiating ACTA balked,[166] and the final provisions did not include graduated response.[167] A weak version of graduated response already existed as part of the safe harbor provisions for service providers in the DMCA,[168] but it was viewed as inadequate by content companies.[169]

Thwarted in the international arena, the administration turned to a different vehicle: private bargains between ISPs and content firms.[170] Then-New York Attorney General Andrew Cuomo brought the two sides together for discussions in 2008,[171] the same year that the Prioritizing Resources and Or-

---

163. *Cf.* Chris Morran, *Movie Studios Claim that Google Fiber Leads to More Piracy*, CONSUMERIST (Dec. 29, 2014), http://consumerist.com/2014/12/29/movie-studios-claim-that-google-fiber-leads-to-more-piracy (discussing survey indicating increase in piracy after Google Fiber deployment in Kansas City).

164. *See* David Kravets, *U.S. Copyright Czar Cozied up to Content Industry, E-mails Show*, WIRED (Oct. 14, 2011, 6:30 AM), http://www.wired.com/2011/10/ copyright-czar-cozies-up.

165. *See* AdamCondeNast, *ACTA Backs away from 3 Strikes*, WIRED (Apr. 21, 2010, 4:10 PM), http://www.wired.com/2010/04/acta-treaty.

166. *See id.*

167. *See* Anti-Counterfeiting Trade Agreement, Oct. 1, 2011, 50 I.L.M. 243 (2011); Annemarie Bridy, *ACTA and the Specter of Graduated Response*, 26 AM. U. INT'L L. REV. 559, 561 (2011).

168. Digital Millennium Copyright Act, 17 U.S.C. § 512(i) (2012); *see* Perfect 10, Inc. v. CCBill L.L.C., 488 F.3d 1102, 1109–13 (9th Cir. 2007); Yu, *supra* note 162, at 1374, 1403–07.

169. *See* Bridy, *supra* note 167, at 572.

170. *See generally* Bridy, *supra* note 160 (discussing interindustry cooperation between rights owners and ISPs).

171. *See* David Kravets, *ISPs To Disrupt Internet Access of Copyright Scoff-*

ganization for Intellectual Property Act established the office of the Intellectual Property Enforcement Coordinator (IPEC) in the executive branch.[172] President Obama appointed Victoria Espinel as his first IPEC, and the Senate confirmed her on December 4, 2009.[173] She became involved in the six strikes negotiations immediately; on December 22, she received a list of the talking points for Sony Pictures' CEO in the talks.[174] The same month, Vice President Joe Biden convened a copyright enforcement meeting that included law enforcement, the IPEC, and content companies—but not ISPs.[175]

Espinel's role became plain by January 2010, when Alec French, the vice president of government relations at NBC Universal, asked her for help with "the cajole set of issues" in the bargaining with ISPs over graduated response.[176] French was close enough to Espinel that he sent the request to her personal e-mail address.[177] Espinel met with representatives of the Recording Industry Association of America, the Motion Picture Association of America (MPAA), and NBC Universal in September 2010 about the project; the meeting invitation from Espinel noted that it was on the birthday of one of the MPAA

---

laws, WIRED (July 7, 2011, 11:08 AM), http://www.wired.com/2011/07/disrupting-internet-access.

172. Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. No. 110-403, § 301, 122 Stat. 4256, 4264–66 (codified as amended at 15 U.S.C. § 8111 (2012)).

173. *See Victoria Espinel*, WHITE HOUSE BLOG, https://www.whitehouse.gov/blog/author/victoria-espinel (last updated July 15, 2013, 7:33 AM).

174. *See* E-mail from DeDe Lea to Victoria Espinel (Dec. 22, 2009), *in* EXHIBIT 8: REDACTED FOIA DOCUMENTS 1, 60 (Apr. 27, 2012) http://blogs.law.harvard.edu/infolaw/files/2012/07/Soghoian_Redacted_Docs.pdf. The e-mail to Espinel was released in response to a Freedom of Information Act (FoIA) request by privacy researcher Chris Soghoian for documents about the Obama administration's involvement in the negotiations. *See* Soghoian v. Office of Mgmt. & Budget, 932 F. Supp. 2d 167 (D.D.C. 2013). Disclosure: the author represented Soghoian in his FoIA suit against Office of Management and Budget (OMB).

175. *See* John M. Owen, Note, *Graduated Response Systems and the Market for Copyrighted Works*, 27 BERKELEY TECH. L.J. 559, 585–86 (2012).

176. *See* E-mail from Alec French to Victoria Espinel (Jan. 6, 2010), *in* REDACTED FOIA DOCUMENTS, *supra* note 174, at 59 (asking for a short call "to explore important development related to graduated response, and directly related to the cajole set of issues"). French held his position at NBC from 2005 to 2010. *Alec French, Esq.*, THORSEN FRENCH ADVOC., http://thorsen-french.com/alecfrench.shtml (last visited Oct. 14, 2015).

177. *See* E-mail from Victoria Espinel to Alec French (Jan. 6, 2010), *in* REDACTED FOIA DOCUMENTS, *supra* note 174, at 60 (Espinel explaining "[I] only check my gmail intermittently now so much quicker to reach me on omb [sic] email").

executives.[178] And, in November 2010, Universal Music sent the ISPs' proposed version of the agreement to Espinel.[179] IPEC was plainly on Hollywood's side. The administration and IPEC did more than just advise, though—they threatened ISPs with unfavorable legislation if the firms failed to reach a voluntary deal,[180] part of a long track record of pro-copyright owner policy.[181]

The providers took the hint, agreeing to a Copyright Alert System, popularly titled "six strikes," in mid-2011.[182] Espinel trumpeted the deal in a post to the White House blog.[183] In short, the Obama administration achieved through jawboning that which it was unable to get through international law.[184]

E. NETWORK NEUTRALITY: "I AM NOT A DINGO"[185]

Network neutrality is a hopeful jawboning story. Over the span of a decade, the Federal Communications Commission has moved its efforts to ensure non-discrimination for Internet traffic from jawboning vaguely grounded in non-binding policy statements to formal rulemaking that brings Internet carriage squarely under the Commission's authority.

---

178. Meeting Invitation from Victoria Espinel to James Schuelke, Kathleen Seighman, and Alan Hoffman, *in* REDACTED FOIA DOCUMENTS, *supra* note 174, at 49. The meeting was set for September 7, 2010.

179. E-mail from Matthew Gerson to Victoria Espinel (Nov. 12, 2010), *in* REDACTED FOIA DOCUMENTS, *supra* note 174, at 2 (including the "ISPs' proposed cleanup of the draft agreement").

180. *See* Jason Mick, *Obama Conscripts ISPs as "Copyright Cops," Unveils "Six Strikes" Plan*, DAILYTECH (July 8, 2011), http://www.dailytech.com/Obama+Conscripts+ISPs+as+Copyright+Cops+Unveils+Six+Strikes+Plan/article22107.htm.

181. *See* Greg Sandoval, *Exclusive: Top ISPs Poised To Adopt Graduated Response to Piracy*, CNET (June 22, 2011), http://www.cnet.com/news/exclusive-top-isps-poised-to-adopt-graduated-response-to-piracy.

182. *See* Mick, *supra* note 180. The Memorandum of Understanding was signed on July 6, 2011. *See* MEMORANDUM OF UNDERSTANDING, *supra* note 153.

183. *See* Victoria Espinel, *Working Together To Stop Internet Piracy*, WHITE HOUSE BLOG (July 7, 2011), https://www.whitehouse.gov/blog/2011/07/07/working-together-stop-internet-piracy.

184. *See* David Kravets, *Copyright Treaty Is Policy Laundering at Its Finest*, WIRED (Nov. 4, 2009), http://www.wired.com/2009/11/policy-laundering.

185. Tom Risen, *FCC Chairman Tom Wheeler: "I Am Not a Dingo*," U.S. NEWS & WORLD REP. (June 13, 2014), http://www.usnews.com/news/blogs/washington-whispers/2014/06/13/fcc-chairman-tom-wheeler-i-am-not-a-dingo. Wheeler was responding to comedian John Oliver's criticism of his background as a telecommunications industry lobbyist; Oliver proclaimed that hiring Wheeler as FCC Chair was "the equivalent of needing a babysitter and hiring a dingo." *Id.* Thanks to Alan Trammell for this reference.

The path began in rural North Carolina in 2004.[186] The local telecommunications company, Madison River Communications, noted an increase in customers using Voice over Internet Protocol (VoIP) to make long-distance telephone calls.[187] VoIP calls undercut Madison River's profitable long-distance service over the conventional telephone system.[188] The firm turned to self-help: it blocked VoIP traffic on its network.[189] Customers complained to the VoIP provider Vonage and the FCC launched an investigation.[190] Madison River surrendered quickly: on March 3, 2005, the FCC announced a settlement,[191] under which the company would cease blocking VoIP and would pay a voluntary fine of $15,000.[192] Formally, the Commission based its decision on its ability to ensure that common carriers engage in practices that are "just and reasonable."[193] However, since this was the first instance of the FCC regulating blocking of an Internet application, it was not plain that the practice fell within its statutory remit.[194]

The real rationale for the FCC's action against Madison River had emerged a year earlier, in a speech titled "Preserving Internet Freedom: Guiding Principles for the Industry" by Chair Michael Powell.[195] Powell outlined the benefits of Inter-

---

186. Conceptually, it begins in 2003, when Tim Wu coined the term "network neutrality." Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. TELECOMM. & HIGH TECH. L. 141 (2003).

187. *See* Matt Evans, *How a Triad Company Helped Open the Debate over Net Neutrality*, TRIAD BUS. J. BIZBLOG (May 15, 2014), http://www.bizjournals.com/triad/blog/2014/05/how-a-triad-company-helped-open-the-debate-over.html.

188. *Id.*; *see* Daniel A. Lyons, *Internet Policy's Next Frontier: Usage-Based Broadband Pricing*, 66 FED. COMM. L.J. 1, 43 (2013).

189. *See* Lyons, *supra* note 188; Evans, *supra* note 187.

190. *See* Lyons, *supra* note 188; Evans, *supra* note 187.

191. Order, Madison River Commc'ns, L.L.C., No. EB-05-IH-0110 (F.C.C. Mar. 3, 2005).

192. Consent Decree, Madison River Commc'ns, L.L.C., No. EB-05-IH-0110, at 2 (F.C.C. Mar. 3, 2005).

193. *Id.* at 1 n.1 ("All charges, practices, classifications, and regulations for and in connection with such communication service, shall be just and reasonable . . . ." (citing 47 U.S.C. § 201(b) (2000))).

194. *See* Stacey Higginbotham, *A Net Neutrality Timeline: How We Got Here*, GIGAOM (Dec. 21, 2010), https://gigaom.com/2010/12/21/a-net-neutrality-timeline-how-we-got-here.

195. Michael K. Powell, Chairman, FCC, Preserving Internet Freedom: Guiding Principles for the Industry, Speech at the University of Colorado School of Law Silicon Flatirons Symposium (Feb. 8, 2004); *see* Richard S. Whitt, *Evolving Broadband Policy: Taking Adaptive Stances To Foster Optimal Internet Platforms*, 17 J. COMM. L. & POL'Y 417, 505–06 (2009). *See generally* Barbara van Schewick, *Network Neutrality and Quality of Service: What a*

net freedom, noting that most providers already offered open access to their customers.[196] He pledged to be vigilant, though, to "keep a sharp eye on market practices."[197] To offer Internet firms a "clear road map," he challenged them to preserve four "Internet Freedoms": freedom to access content, use applications, attach personal devices, and obtain service plan information.[198] While the FCC nominally grounded its enforcement action in its authorizing statute, the truth is that "Madison River was the first major case of the FCC going after a company for violating open Internet principles" set out in Powell's speech.[199]

In August 2005, the FCC removed the common carriage rationale for network neutrality regulation by reclassifying wireline broadband Internet access as an information service.[200] Instead, the Commission adopted—on the same day—a statement of principles putatively based upon a congressional directive to encourage broadband deployment, but in fact enacting Powell's Internet Freedoms as policy.[201] There were four expressly non-binding[202] principles. First, consumers could access all lawful Internet content. Second, users could run applications and services subject to law enforcement needs. Third, customers could connect to legal devices that did not harm the network. Finally, Americans should enjoy competition among providers of networks, applications, services, and content.[203]

The FCC did not have to wait long to test its policy state-

Nondiscrimination Rule Should Look Like, 67 STAN. L. REV. 1 (2015); Tejas N. Narechania, *Federal and State Authority for Network Neutrality and Broadband Regulation*, 17 STAN. TECH. L. REV. (forthcoming 2015).

196. Powell, *supra* note 195, at 3.

197. *Id.*

198. *Id.* at 5–6.

199. *See* Aaron Sankin, *The Worst Net Neutrality Violations in History*, DAILY DOT (May 21, 2014), http://www.dailydot.com/politics/net-neutrality-violations-history.

200. Report and Order and Notice of Proposed Rulemaking, *In re* Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, 20 F.C.C. Rcd. 14,853, 14,857 (2005).

201. Policy Statement, *In re* Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, C.C. Docket No. 02-33, at 2 (F.C.C. Aug. 5, 2005); *see* 47 U.S.C. § 1302(a) (2012) (incorporating the Telecommunications Act of 1996 and directing FCC to "encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans").

202. Policy Statement, *In re* Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, C.C. Docket No. 02-33, at 3 n.15 ("[W]e are not adopting rules in this policy statement.").

203. *Id.* at 3.

ment. In 2007, Comcast customer Robb Topolski noticed he was having trouble using the BitTorrent peer-to-peer application despite his speedy broadband connection.[204] The technologically-talented Topolski ran tests that confirmed his troubles: Comcast was deliberately interfering with BitTorrent to slow its use.[205] The public interest groups Free Press and Public Knowledge filed complaints with the FCC, which moved to investigate.[206] At a Senate committee hearing the following April, FCC Chair Kevin Martin rejected calls for network neutrality legislation, noting that the 2005 open Internet policy statement enabled the Commission to act on a case-by-case basis—a claim disputed by senators on the committee.[207] In August 2008, the FCC moved to prohibit Comcast's interference with peer-to-peer traffic.[208] While the Commission dutifully cited its ancillary statutory authority as one set of grounds for the enforcement action, the first authority it pointed to was the 2005 statement[209]—and the FCC noted the case was about "authority to enforce federal *policy*," rather than any statutory grant.[210] Comcast appealed the agency's decision to the D.C. Circuit Court of Appeals, which ruled that a policy statement was insufficient basis for enforcement, since policies "[were] not delegations of regulatory authority."[211] Moreover, the FCC's claims to ancillary authority failed for lack of a predicate: the agency did not identify any statutory power to which its operations were tied.[212] The anti-throttling order was reversed.

While the *Comcast* case proceeded in the D.C. Circuit, the FCC moved once again to make its policy mandates more closely tied to its formal authority. In October 2009, the Commission

---

204. *See* Peter Eckersley et al., *Packet Forgery by ISPs: A Report on the Comcast Affair*, EFF (Nov. 28, 2007), https://www.eff.org/wp/packet-forgery-isps-report-comcast-affair.

205. *See id.* Interestingly, the technique Comcast used is quite similar to the one that China's Great Firewall employs. *See Bulletin 05: Probing Chinese Search Engine Filtering*, OPENNET INITIATIVE, (Aug. 19, 2004), https://opennet.net/bulletins/005 (describing use of RST packets at TCP level).

206. Memorandum Opinion and Order, Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications, No. EB-08-IH-1518, at 5 (F.C.C. Aug. 1, 2008) [hereinafter Formal Complaint of Free Press].

207. *See* Grant Gross, *FCC's Martin: Comcast Blocking Was Widespread*, MACWORLD (Apr. 22, 2008), http://www.macworld.com/article/1133112/comcast_p2p.html.

208. Formal Complaint of Free Press, *supra* note 206, at 1.

209. *Id.* at 7–17.

210. *Id.* at 15 (emphasis added).

211. Comcast Corp. v. FCC, 600 F.3d 642, 654 (D.C. Cir. 2010).

212. *Id.* at 658–61.

proposed open Internet rules to be a "codification of the existing Internet policy principles" along with "additional principles of nondiscrimination and transparency"[213] based on its statutory powers under Section 706(a) of the Telecommunications Act of 1996.[214] After receiving public comments, the FCC adopted the rules as its Open Internet Order in December 2010.[215] While the Commission linked its policy prescriptions to a specific grant of statutory authority, its effort was nonetheless challenged before the D.C. Circuit, this time by Verizon.[216] The Court of Appeals agreed with the Commission that it had authority under Section 706(a) to regulate net neutrality[217]—a significant victory for the FCC—but rejected the anti-discrimination and anti-blocking rules.[218] The D.C. Circuit found that these rules effectively treated network providers as common carriers, contrary to the FCC's earlier decisions to remove providers from the common carriage regime of Title II.[219]

To effectuate the principles first outlined by Powell in 2004, the FCC would have to go the last mile for net neutrality: reclassifying broadband Internet service as subject to Title II.[220] FCC Chair Tom Wheeler sought to do just that—proposing the "FCC use its Title II authority to implement and enforce open internet protections."[221] The full Commission voted to adopt his proposal on February 26, 2015.[222] Thus, with network neutrali-

213. Notice of Proposed Rulemaking, Preserving the Open Internet, G.N. Docket No. 09-191, at 4 (F.C.C. Oct. 22, 2009).

214. *Id.* at 36–37.

215. Report and Order, Preserving the Open Internet, G.N. Docket No. 09-191 (F.C.C. Dec. 21, 2010).

216. *See* Andrew Crocker, Verizon v. FCC*: Verizon Challenges FCC's Open Internet Order*, JOLT DIGEST (July 10, 2012), http://jolt.law.harvard.edu/digest/telecommunications/verizon-v-fcc.

217. Verizon v. FCC, No. 11-1355, slip op. at 17 (D.C. Cir. 2014) ("[W]e start and end our analysis with section 706 of the 1996 Telecommunications Act, which . . . furnishes the Commission with the requisite affirmative authority to adopt the regulations.").

218. *Id.* at 63.

219. *Id.* at 45–60.

220. *See id.* at 10–12; John Blevins, *A Fragile Foundation—The Role of "Intermodal" and "Facilities-Based" Competition in Communications Policy*, 60 ALA. L. REV. 241, 252 n.42 (2009).

221. Wheeler, *supra* note 3.

222. *See* Julianne Pepitone, *FCC Passes Net Neutrality Rules in Victory for Open-Internet Activists*, NBC NEWS (Feb. 26, 2015), http://www.nbcnews.com/tech/tech-news/fcc-passes-net-neutrality-rules-victory-open-internet-activists-n313301; Tom Wheeler, *Good News for Consumers, Innovators and Financial Markets*, FCC: OFFICIAL FCC BLOG (Feb. 26, 2015), https://www.fcc.gov/blog/good-news-consumers-innovators-and-financial-markets (announcing adoption of rules).

ty, the FCC has gradually shifted from jawboning—enforcement based on an official's speech, sparsely grounded in statute—to full-fledged rulemaking within the FCC's statutory powers.[223]

The FCC's net neutrality enforcement efforts show encouraging improvements in legitimacy over time. They offer a useful case study both of jawboning's edges and of how state actors can make their conduct more legitimate. At first, the FCC used informal enforcement of its general common carriage rules to force a quick settlement with Madison River, even though the Commission would remove any force common carriage had a few months later. Now, the Commission has adopted, through formal rulemaking, a scheme that subjects Internet access and carriage to classic Title II common carriage. Those rules are certain to be challenged in court, but from the perspective of legitimacy, that is a benefit rather than a drawback: by proceeding (albeit reluctantly) to move net neutrality under the shield of Title II, the FCC has helped regulated entities to obtain both clarity and accountability. This is a lesson other state actors could learn from.

This Part has documented the rise in jawboning as a tactic employed by government to press Internet platforms to carry out the state's wishes. It is a popular method for regulators, especially when their formal authority is constrained. Jawboning often occurs out of the limelight, and can be difficult (or at least quite costly) to resist. Next, the Article turns to a normative evaluation of jawboning and other government enforcement methods.

II. A TAXONOMY OF GOVERNMENT PRESSURES AND THEIR LEGITIMACY

This Part seeks to define when governmental pressures on Internet platforms are, or are not, legitimate. First, it places the Article's argument in context by explaining why Internet intermediaries are highly vulnerable to informal pressures from state actors. Next, it builds a taxonomy of government pressures along two dimensions: compulsion and authority. Then, it offers two methodologies—one grounded in constitutional structure, the other in process-based approaches to governance—to assess the legitimacy of jawboning, and to explain why this type of government action should be censured.

---

223. The Commission's power to classify broadband as under, or outside, Title II was confirmed by the Supreme Court in *Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967 (2005).

A. KNUCKLING UNDER

Internet platforms are the keystone species of the online ecosystem, and like those species, they are vulnerable to pressures.[224] Platforms connect content creators with readers and listeners.[225] The power and weakness of Internet platforms is that they are intermediaries. Unlike broadcast television stations and record labels of the twentieth century, Internet services carry predominantly if not exclusively content created by others.[226] They help to solve the problem of attention scarcity: users with limited time must decide what drops to drink out of a sea of content.[227] Platforms' choices, though, are of surpassing importance. They determine what information is available, and salient, for consumers. With Google search results, for example, sites not listed on the first two pages rarely receive click-throughs from users.[228] Lower-ranked sites are less visible, and unranked ones are effectively invisible.[229] Accordingly, platform decisions to remove or de-emphasize content have particular force. Unfortunately, platforms are unusually vulnerable to

224. *See* Karl Gruber, *Single Species May Be Key to Reef Health*, AUSTRALIAN GEOGRAPHIC (Sept. 26, 2014), http://www.australiangeographic.com.au/news/2014/09/single-keystone-species-may-be-key-to-reef-health; L. Scott Mills et al., *The Keystone-Species Concept in Ecology and Conservation*, 43 BIOSCIENCE 219, 219 (1993) (defining a keystone species as one whose "presence is crucial in maintaining the organization and diversity of [its] ecological community" and that it is "exceptional, relative to the rest of the community, in [its] importance").

225. *See* Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 432 (2009).

226. *Cf.* Kreimer, *supra* note 57, at 16–18 ("Unable to reach those who originate or receive communications, official actors have sought to exert pressure on intermediaries . . . .").

227. *See* Michael H. Goldhaber, *The Attention Economy and the Net*, 2 FIRST MONDAY (1997), http://firstmonday.org/article/view/519/440.

228. While studies vary in precise details, nearly all show a powerful relationship between placement in Google's search results and click-through rates (the rate at which a search user clicks a given result). *See, e.g.*, Danny Goodwin, *Top Google Result Gets 36.4% of Clicks [Study]*, SEARCH ENGINE WATCH (Apr. 21, 2011), http://searchenginewatch.com/sew/news/2049695/top-google-result-gets-364-clicks-study (noting a study that found "ranking beyond Page 2 . . . has almost no business value"); Eric Siu, *24 Eye-Popping SEO Statistics*, SEARCH ENGINE J. (Apr. 19, 2012), http://www.searchenginejournal.com/24-eye-popping-seo-statistics/42665 ("[Seventy-five percent] of users never scroll past the first page of search results.").

229. *See* Barry Schwartz, *A New Click Through Rate Study for Google Organic Results*, MARKETING LAND (Oct. 1, 2014, 3:09 PM), http://www.marketingland.com/new-click-rate-study-google-organic-results-102149; *see also* David Segal, *The Dirty Little Secrets of Search*, N.Y. TIMES (Feb. 12, 2011), http://www.nytimes.com/2011/02/13/business/13search.html (discussing J.C. Penney's attempt to artificially increase its rank in Google search results).

government pressures, both formal and informal.

Platforms' gatekeeping function makes them a natural target for enforcement.[230] It is far easier and more effective to impose controls upon an intermediary than upon a host of dispersed speakers who may be difficult to identify, located outside the regulators' jurisdiction, or judgment-proof.[231] Platforms draw attention because government actors have scarce resources too and want the greatest effect for a given investment in enforcement. Furthermore, online information by default does not follow geographic or jurisdictional boundaries.[232] A platform will typically be subject to the actions of an array of regulators. For example, where state officials are empowered to enforce intellectual property laws such as trade secret theft, intermediaries must expect to come under the supervision of state attorneys general in addition to federal actors who enforce copyright and anti-counterfeiting statutes.[233]

Externalities also create skewed incentives for platforms. Firms that host disfavored content reap little benefit, since any single user or source generates but tiny revenue for the platform.[234] However, they face the full force of any legal liability or public disapprobation that attends that material.[235] The cost-benefit calculus is clear: it makes sense to censor anything questionable.[236] The problem worsens with content that represents a minority viewpoint: the return from keeping it online is further diminished, and appeals by government or dissatisfied civil society groups may have greater appeal (and hence greater cost to the platform) from the majority of users.[237]

Moreover, platforms face a powerful information asymmetry that compounds the economic bias towards censorship. They have far less information about whether content is lawful, or disreputable, than the creator does, and investigation to gain that knowledge can be costly at scale.[238] Here, too, the cost-

230. *See* Kreimer, *supra* note 57, at 17.

231. *See* Mann & Belzley, *supra* note 55, at 259.

232. *See* Alan M. Trammell & Derek E. Bambauer, *Personal Jurisdiction and "teh Interwebs*," 100 CORNELL L. REV. (forthcoming 2015) (manuscript at 27).

233. *See, e.g.*, 18 U.S.C. § 1832 (2012); NEV. REV. STAT. ANN. § 600A.035 (West 2015) (imposing criminal penalties for theft of trade secrets).

234. *See* Kreimer, *supra* note 57, at 28–29.

235. *See id.*

236. *See id.* at 29–30.

237. *See id.* at 28–29.

238. *See id.* at 69–70; *cf.* Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1035–36 (2014) (discussing information asymmetries for

benefit analysis favors complying with pressures to remove content rather than to resist or obtain more information.[239] Where the platform creates the content, it bears the full weight of decisions to delete or promote it, but where others do so, it only bears the marginal cost of that author's favor or popularity in doing so.[240] This is especially true with minority viewpoints, such as LGBT content, where hosting the material is likely neither profitable nor popular.[241]

There might be a market niche for firms that vow to resist jawboning.[242] However, it is hard to credibly signal that commitment, particularly since firms effectively must comply with some content removal requirements to stay within the ambit of safe harbors for copyright infringement, trademark infringement, child pornography violations, and the like.[243] It is possible to generate such a signal—Ripoff Report has upheld its pledge not to remove user-posted reviews, at the cost of considerable litigation—but it is difficult.[244]

The statutes and doctrinal developments protecting platforms that take sufficient precautions, such as removing content that allegedly infringes intellectual property rights upon notification, are a two-edged sword.[245] The safe harbors themselves relieve platforms from liability risk, but compliance with them also demonstrates that intermediaries are capable of filtering content.[246] This creates a slippery slope: Internet services that can remove content-infringing copyright upon notice can presumably also disable access to revenge porn,[247] defamation,[248] hate speech,[249] pornography,[250] threats,[251] and other un-

producers and consumers of software).

239. *See* Kreimer, *supra* note 57, at 28–30.

240. *See id.* at 38–41.

241. *See id.*

242. *See* Lichtman & Posner, *supra* note 55, at 241–43 (arguing that the imposition of ISP liability is a desirable option despite the fact it may create positive externalities).

243. *See supra* notes 84–86.

244. *See, e.g.*, Small Justice L.L.C. v. Xcentric Ventures, No. 13-cv-11701, 2014 WL 1214828, at *9–10 (D. Mass. Mar. 24, 2014) (denying partially a motion to dismiss copyright claims based upon the Ripoff Report).

245. *See* 17 U.S.C. § 512(c) (2012) (stating that service providers are not liable for copyright infringments committed by their users if the service providers are unaware of the violations).

246. *See also id.*; 47 U.S.C. § 230(c)(2) (2012).

247. *See* Franks, *supra* note 43, at 688–89.

248. *See* Anita Bernstein, *Real Remedies for Virtual Injuries*, 90 N.C. L. REV. 1457, 1485 (2012).

249. *See* Danielle Keats Citron & Helen Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*, 91 B.U. L. REV.

savory material. As a legal matter, platforms can point to statutory and common law safe harbors as the reasons for their removal of content, but refusing to filter other material becomes more difficult as a practical matter (they clearly have the capabilities) and as a normative one (is copyright infringement worse than hate speech?).[252] In addition, some firms, such as Google, engage in additional filtering. They remove child porn, terrorism sites, and sensitive personal information from results, even though the law does not compel or encourage them to do so.[253] These voluntary efforts, while likely laudable, further limit platforms' moral basis for refusing to engage in further removals.

Put crudely, Internet platforms face structural incentives to knuckle under government jawboning over content.

B. A TAXONOMY OF PRESSURES

Government pressures can be usefully mapped along two dimensions: authority and compulsion. This Article argues that informal pressures on Internet platforms by government become problematic as the state's actions increase in compulsion, decrease in authority, or both. First, as the level of compulsion of the state's effort to influence the platform increases, that effort becomes more potentially problematic. The ends of the continuum are clear. At one pole, the state expresses its opinion or position without consequence—it evinces a preference for how the platform ought to behave, but its statements are hortatory.[254] At the other pole, the state's views are backed by an overt threat of action that will have material consequences for the ISP.[255] As the government's command is backed by greater force, it is more suspect—or, put another way, requires greater justification.

Second, as the legal basis for the state's actions becomes less certain, those efforts become more potentially problematic.

1435, 1468–69 (2011).

250. *See* Preston, *supra* note 63.

251. *See* Citron & Norton, *supra* note 249.

252. See *id.* at 1453–54.

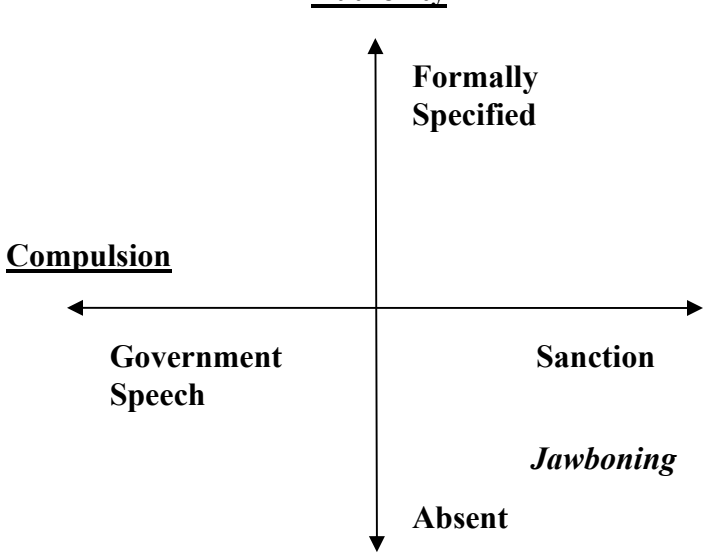
253. *Google and Microsoft Agree to Steps To Block Abuse Images*, BBC NEWS (Nov. 18, 2013), http://www.bbc.com/news/uk-24980765; *Removal Policies*, GOOGLE, https://support.google.com/websearch/answer/2744324?hl=en (last visited Oct. 14, 2015); *Google Reveals "Terrorism Video" Removals*, BBC NEWS (June 17, 2012), http://www.bbc.com/news/technology-18479137.

254. Speech may have negative reputational consequences, but like criticism of other varieties, that type of injury is not troublesome here.

255. *See supra* notes 21–27 and accompanying text.

Here, too, the extremes of the spectrum are in clear focus. When the state operates on the basis of clear legal authority, as when the Environmental Protection Agency bargains with a polluter who has violated the Clean Water Act, informal resolution is not only untroubling, but often desirable.[256] And when the state operates utterly without authority, as when law enforcement deliberately violates the rights of an innocent person, those actions are ultra vires and undoubtedly illegitimate.[257]

The middle range is challenging to map for both dimensions. Any metric is vulnerable to question.[258] However, the principle that this taxonomy develops is important: the more pressure the state applies, and the greater the stakes that accompany disobeying its wishes, the more those actions need scrutiny and justification. As a given pressure from the state involves greater compulsion and lesser authority, it is increasingly likely to constitute jawboning. Overall, the mapping looks like so:



256. *See Civil Cases and Settlements by Statute: Clean Water Act*, U.S. ENV'T PROT. AGENCY, http://cfpub.epa.gov/enforcement/cases/index.cfm (last updated Oct. 1, 2015) (showing that the vast majority of Clean Water Act violations are decided informally).

257. *See, e.g.*, *In re* Gault, 387 U.S. 1, 28–31 (1967) (reversing the dismissal of a petition for a writ of habeas corpus after finding defendant's due process rights were blatantly violated); *see generally* Jane R. Bambauer & Toni M. Massaro, *Outrageous and Irrational*, 100 MINN. L. REV. 281 (2015).

258. *See generally* Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377, 411–17 (2009) [hereinafter Bambauer, *Cybersieves*] (describing multiple metrics).

Figure 1 - Taxonomy of Pressures

Examples may helpfully illustrate the schematic above. In the top right quadrant, the state is using well-defined regulatory authority to impose penalties, such as fines or incarceration, upon targets who have notice of these potential sanctions to guide their conduct. This set of activities represents, hopefully, the vast majority of state enforcement pressures.[259] Putting aside concerns about the level of sanctions and the evenness of enforcement, government action in this quadrant is conventional and desirable. And those potential problems—unduly harsh penalties or discriminatory enforcement—are mitigated by constitutional doctrines such as equal protection,[260] due process,[261] and the ban on cruel and unusual punishment.[262]

The upper left quadrant denotes forbearance by the state. Here, government can rely upon properly created and delineated authority, but decides to respond with less compulsory measures. The state may be forced to rely on lesser methods due to resource constraints—it is practically impossible to audit every tax return, but the Internal Revenue Service can denounce tax cheats at low cost.[263] Or the government may decide to use suasive rather than punitive measures as a matter of policy, such as when the Obama administration decided not to enforce federal controlled substance laws that ban marijuana in states where the drug is legal under state law.[264] This quadrant

259. *See* Noah, *supra* note 53, at 891–92 (discussing the use of consent decrees as a means of imposing penalties for statutory violations).

260. *See generally* United States v. Armstrong, 517 U.S. 456, 465–66 (1996) (discussing requirements to show selective prosecution based on race).

261. *See* Brady v. Maryland, 373 U.S. 83 (1963) (holding that suppression of evidence by the prosecuting attorney was a violation of due process).

262. *See* Roper v. Simmons, 543 U.S. 551 (2005) (ruling that imposing the death penalty on minors is cruel and unusual punishment).

263. *See, e.g.*, *Chances of IRS Tax Audit Are Lowest in Years*, CBS MONEYWATCH (Apr. 13, 2014), http://www.cbsnews.com/news/chances-of-irs-tax-audit-are-lowest-in-years ("Budget cuts and new responsibilities are straining the Internal Revenue Service's ability to police tax returns."); *Anti-Tax Law Evasion Schemes*, INTERNAL REVENUE SERV., (Oct. 24, 2014), http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Anti-Tax-Law-Evasion-Schemes-Introduction (describing kit designed to "educate the public about abusive tax avoidance schemes").

264. Controlled Substance Act, 21 U.S.C. §§ 801–89; U.S. DEP'T OF JUSTICE, MEMORANDUM FROM JAMES M. COLE TO ALL U.S. ATTORNEYS (Aug. 29, 2013), http://www.justice.gov/iso/opa/resources/305201382913275685746 7.pdf.

describes government action that utilizes less stringent measures than it is authorized to undertake.

The lower left quadrant is characterized by speech, counterspeech, or wishful thinking. Here, the government is employing measures that rely on prodding rather than penalties. President Obama's criticism of *Citizens United v. FEC* at his 2010 State of the Union address, with the members of the Supreme Court in the audience, provides one exemplar.[265] The president has no power to alter the Court's decisions about the scope of the First Amendment, but he can upbraid the justices. Non-binding congressional resolutions over the nation's foreign policy are another instance.[266] State actions in this zone possess both minimal authorization and minimal consequences. There may be some risk of overreaction to governmental suasion here, but that overreaction can be corrected with little concern for repercussion.

The last type of pressure, found in the bottom right quadrant, is the most dangerous kind: it is where the state operates by threatening or imposing penalties that lack grounding in law. This is where jawboning resides. Examples of this type of conduct are less infrequent than one would hope. A San Francisco police sergeant arrested a public defender in a courthouse hallway for advising her client not to answer his questions; the chief of police subsequently defended the sergeant's actions.[267] President George W. Bush authorized the National Security Agency to conduct surveillance on Americans' international telephone calls and e-mail traffic without obtaining either a Title III warrant or an order under the Foreign Intelligence Surveillance Act.[268] Boston police officers arrested a man who recorded

265. Office of the Press Secretary, *Remarks by the President in State of the Union Address*, WHITE HOUSE (Jan. 27, 2010), http://www.whitehouse.gov/the-press-office/remarks-president-state-union-address; *see* Adam Liptak, *A Rare Rebuke, in Front of a Nation*, N.Y. TIMES, Jan. 29, 2010, at A12.

266. *See, e.g.*, *Hill Challenges Reagan on Persian Gulf Policy*, 43 CQ ALMANAC 252 (1987), http://library.cqpress.com/cqalmanac/cqal87-1144869 (discussing congressional efforts to pass a non-binding resolution delaying a Reagan-led Persian Gulf policy).

267. *See* Alex Emslie, *S.F. Police Chief: Arrested Public Defender Won't Be Charged*, KQED (Feb. 5, 2015), http://ww2.kqed.org/news/2015/02/05/s-f-police-chief-arrested-public-defender-wont-be-charged; *Public Defender Attorney Arrested Last Week Says San Francisco Police Chief Apologized*, SAN JOSE MERCURY NEWS (Feb. 6, 2015), http://www.mercurynews.com/crime-courts/ci_27473625/public-defender-attorney-arrested-last-week-says-san.

268. 18 U.S.C. § 2516 (2012) (Wiretap Act warrant); 50 U.S.C. § 1804(a) (2012) (FISA order); *see generally* Leslie Cauley, *NSA Has Massive Database*

them with his cell phone camera while they were punching a man in the middle of Boston Common.[269] Government officials and agents do bad things sometimes—they act with force or compulsion even when they clearly lack authority to do so. Here is where the state's actions are increasingly illegitimate; they are not the product of legal authority, and hence are neither transparent nor accountable. The precise relationship between the variables—how decreasing authority and increasing sanction interact to produce a given level of legitimacy—is unclear.[270] The mapping is a heuristic, not a mathematical plot. Greater sanctions, when backed by questionable authority, might be more legitimate than minor sanctions where a foundation in law is completely lacking, or the reverse might be true. Regardless of the exact formula, legitimacy generally decreases as the state employs greater penalties and as its legal foundation becomes less established.

This taxonomy usefully maps governmental pressures on Internet platforms. Legitimacy will increase as the state's authority is increasingly formally specified, such as in statutes, binding judicial decisions, or properly-promulgated administrative regulations. The constraints of both formal rulemaking, such as the Administrative Procedures Act,[271] and judicial review create accountability for regulators[272] and push them to specify permitted and proscribed conduct with sufficient narrowness.

---

of Americans' Phone Calls, USA TODAY (May 11, 2006), http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm; James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/16program.html.

269. Glik v. Cunniffe, 655 F.3d 78, 85, 88 (1st Cir. 2011) (holding not only that the arrest violated Simon Glik's rights under the First and Fourth Amendments, but that the officers involved were not entitled to qualified immunity, since those rights were clearly established).

270. Government actors might use lesser force or sanctions if they are aware that the justification for their actions is in question, or they might use greater force as a means of compensating psychologically. *Cf.* Brigham Daniels, *When Agencies Go Nuclear: A Game Theoretic Approach to the Biggest Sticks in an Agency's Arsenal*, 80 GEO. WASH. L. REV. 442, 450, 454 (2012) (arguing that government agencies use threats of large regulatory penalties to broadly influence the regulation landscape).

271. 5 U.S.C. §§ 500–596(e) (2012).

272. *See generally* Chevron U.S.A. v. Nat. Res. Def. Council, 467 U.S. 837 (1984); SEC v. Chenery, 332 U.S. 194 (1947); Kevin M. Stack, *The Constitutional Foundations of* Chenery, 116 YALE L.J. 952 (2007).

Similarly, legitimacy rises as the strength of the enforcement sanction diminishes. The costs of error are simply lower, and erroneous decisions on content restrictions impose real harms.[273] Since no process of review is perfect, some errors will persist, thus sacrificing accountability for those incorrectly targeted.[274] There are also costs to underenforcement, but this scale is a relative measure.[275] Legitimacy regarding compulsion can be thought of as analogous to the rule of lenity in criminal law: when comparing sanctions in a given case, the one marginally less severe is likely to be more legitimate.[276]

Regulation by the state can be helpfully categorized based on specification of authority and level of compulsion. Where authority is vague and compulsion is high, the government is engaged in jawboning.

C. ASSESSING LEGITIMACY

Assessing the legitimacy of government actions to regulate information is challenging, but there are at least two different methodologies that indicate jawboning does not pass muster. The first looks to the jurisprudence and norms around the First Amendment. The second employs a process-based framework used to evaluate governance of online censorship. Both find that jawboning tends to lack legitimacy.

1. First Amendment Limits and Values

The First Amendment is both a substantive source of restrictions upon governmental action and an expression of deeply-held societal values.[277] Both as doctrine and norm, the First Amendment means that the United States treats speech regulations differently than other legal rules—in particular, regimes that limit speech are generally viewed with skepticism.[278]

---

273. *See* Kreimer, *supra* note 57, at 27–33.

274. *See id.*

275. *See* Bambauer, *Cybersieves*, *supra* note 258, at 396–99.

276. *See* United States v. Bass, 404 U.S. 336, 347 (1971) (stating that ambiguous criminal statutes "should be resolved in favor of lenity"). *See generally* Zachary Price, *The Rule of Lenity as a Rule of Structure*, 72 FORDHAM L. REV. 885 (2004); Note, *The New Rule of Lenity*, 119 HARV. L. REV. 2420 (2006).

277. *See* Robert Post, *Reconciling Theory and Doctrine in First Amendment Jurisprudence*, 88 CAL. L. REV. 2353, 2368 (2000).

278. *See, e.g.*, United States v. Stevens, 559 U.S. 460, 470 (2010) ("The First Amendment's guarantee of free speech does not extend only to categories of speech that survive an ad hoc balancing of relative social costs and benefits. The First Amendment itself reflects a judgment by the American people that

When government regulates optometrists[279] or teeth whitening[280] or casket sales,[281] its efforts enjoy almost complete deference from judicial review. Only the most blatantly irrational decisions are subject to reversal.[282] By contrast, laws directed at speech generally draw heightened scrutiny, and regulations aimed at specific content face strict scrutiny and near-certain invalidation.[283] Federal and state governments alike have found clever means to circumvent the restrictions that the First Amendment places upon their abilities to regulate speech because of its content, from funding to the use of putatively unrelated laws to a range of informal pressures.[284] Those workarounds, however, drive home the point: the background legal rule and societal norm is that government regulation of speech is presumptively suspect. A second-order result of this presumption against speech regulation is that rules restricting content must be relatively clear and well-defined. Ambiguity in what material falls within a rule's proscription is usually fatal.[285]

The First Amendment importantly constrains the powers of the state. The federal government is not only an organ of enumerated and limited powers, but it must exercise those powers subject to the First Amendment's dictates.[286] This approach, exemplified by the work of Philip Hamburger, treats

---

the benefits of its restrictions on the Government outweigh the costs.").

279. *See* Williamson v. Lee Optical of Okla., Inc., 348 U.S. 483 (1955).

280. *See* N.C. Bd. of Dental Exam'rs v. FTC, 135 S. Ct. 1101 (2015); *see* Adam Liptak, *Regulatory Case in North Carolina Appears To Trouble Supreme Court*, N.Y. TIMES, Oct. 15, 2014, at A24.

281. *See* St. Joseph Abbey v. Castille, 712 F.3d 215 (5th Cir. 2013).

282. *See id.* at 226; *see* Bambauer & Massaro, *supra* note 257 (discussing outrageous and irrational government conduct).

283. *See* Brown v. Entm't Merchs. Ass'n, 131 S. Ct. 2729, 2738 (2011) ("Because the [challenged] Act imposes a restriction on the content of protected speech, it is invalid unless California can demonstrate that it passes strict scrutiny—that is, unless it is justified by a compelling government interest and is narrowly drawn to serve that interest."). *See generally* United States v. Carolene Prods. Co., 304 U.S. 144, 152 n.4 (1938) ("There may be narrower scope for operation of the presumption of constitutionality when legislation appears on its face to be within a specific prohibition of the Constitution, such as those of the first ten amendments . . . .").

284. *See* Bambauer, *Orwell's Armchair*, *supra* note 58.

285. *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844, 870–74 (1997).

286. *See* Philip Hamburger, *Getting Permission*, 101 NW. U. L. REV. 405, 416–20 (2007) (arguing that licensing speech and the press "dispossesses an independent people of their individual authority and renders them subservient").

the Amendment principally as a check upon government rather than as an individual entitlement conferred upon citizens.[287] Constraining the government's ability to regulate speech is useful, and desirable, even if no one speaks. The distinction between limit and entitlement is that individual entitlements can be reallocated as the holders think best, but limits have been societally determined and cannot be unilaterally shifted.[288] This approach suggests that governmental attempts to exceed those limits are not legitimate, even if they escape constitutional sanction by reviewing courts.[289]

First Amendment doctrine has at times been attentive to informal and indirect regulations of speech. For example, the Supreme Court invalidated a Minnesota tax on paper and ink used in publishing newspapers.[290] The Court noted that the tax singled out the press for special—and negative—treatment.[291] Moreover, the sizable exemption built into the tax code meant that only a few Minnesota publishers were effectively subject to the levy; the state seemed to have targeted a subgroup of the press.[292] The Court dealt similarly with a Louisiana tax on newspapers with circulation greater than 20,000 copies per week,[293] and with an Arkansas sales tax scheme that exempted magazines on certain subjects.[294]

Skepticism about informal modes of enforcement goes beyond taxation. Rhode Island set up a "Commission to Encourage Morality in Youth" to review publications for obscenity and indecency.[295] When the Commission determined that a piece of printed matter was not suitable for consumption by minors, it

287. *See* Hamburger, *supra* note 58, at 484; Hamburger, *supra* note 286; Philip Hamburger, *The New Censorship: Institutional Review Boards*, 2004 SUP. CT. REV. 271, 276–81 (2004) [hereinafter Hamburger, *Censorship*].

288. Hamburger, *supra* note 58, at 484 ("[C]onstitutional rights are communally imposed legal limits, and the federal government therefore cannot free itself from these limits by making side deals with private or state actors.").

289. Hamburger, *Censorship*, *supra* note 287. *See generally* Bambauer, *Orwell's Armchair*, *supra* note 58 (discussing censorship methods available to U.S. governments despite First Amendment restrictions).

290. Minneapolis Star & Tribune Co. v. Minn. Comm'r of Revenue, 460 U.S. 575, 579 (1983).

291. *Id.* at 582–83.

292. *Id.* at 591–92.

293. Grosjean v. Am. Press Co., 297 U.S. 233, 251 (1936).

294. Ark. Writers' Project, Inc. v. Ragland, 481 U.S. 221, 227–34 (1987).

295. *See* Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 59–60 (1963).

would notify distributors by letter, asking for their cooperation in removing the material from circulation.[296] While the Commission itself lacked enforcement power, its letters invariably noted that the body could suggest targets for prosecution to the Attorney General.[297] The Supreme Court invalidated the statute establishing the Commission, noting that "informal censorship may sufficiently inhibit the circulation of publications to warrant injunctive relief."[298] The Court's admonition that "freedoms of expression must be ringed about with adequate bulwarks"[299] has led to the development of buffer zones even around unprotected content such as defamation,[300] obscenity,[301] and incitement.[302] These cases suggest that the Court patrols, at least occasionally, for indirect means of regulating speech.

The doctrine and norms of the First Amendment suggest why jawboning is particularly problematic in the context of Internet information: state actions that would be unexceptional in other contexts can be illegitimate when they touch speech.[303] The Constitution sets the default for efforts to regulate information: governments must justify their attempts to do so. They routinely overreach with speech-related laws and rules; indeed, the recent history of Supreme Court First Amendment jurisprudence is a rogue's gallery of popular yet unconstitutional legislation.[304] Private bargains over information take place un-

296. *See id.* at 61–64.

297. *See id.* at 62–63.

298. *Id.* at 67.

299. *Id.* at 66.

300. *See* N.Y. Times v. Sullivan, 376 U.S. 254, 727 (1964); *cf.* Hustler Magazine v. Falwell, 485 U.S. 46, 56 (1988) (prohibiting the award of damages to public figures for intentional infliction of emotional distress unless done with actual malice).

301. *See* Stanley v. Georgia, 394 U.S. 557, 559 (1969) ("[T]he mere private possession of obscene matter cannot constitutionally be made a crime.").

302. *See* R.A.V. v. St. Paul, 505 U.S. 377, 381 (1992) (invalidating an ordinance on the grounds that "it prohibits otherwise permitted speech solely on the basis of the subjects the speech addresses").

303. *See* Hamburger, *Censorship*, *supra* note 287, at 313–21.

304. *See* Brown v. Entm't Merchs. Ass'n, 131 S. Ct. 2729, 2735 (2011) (invalidating a California law forbidding retailers from selling violent video games to minors); Sorrell v. IMS Health, Inc., 131 S. Ct. 2653, 2669 (2011) (invalidating a Vermont statute controlling the use of pharmacy records); U.S. v. Stevens, 559 U.S. 460, 482 (2010) (invalidating a federal law that criminalized the possession or sale of depictions of animal cruelty); *cf.* Snyder v. Phelps, 562 U.S. 443, 458–59 (2011) (holding that the First Amendment protected picketing at a soldier's funeral). *See generally* Ronald K.L. Collins, *Exceptional Freedom—The Roberts Court, the First Amendment, and the New Absolutism*, 76

der circumstances lacking not only judicial review, but also the constraints and trade-offs of the legislative or administrative rulemaking processes. Attempts to regulate speech often fail during the legislative or administrative agency process, and when they succeed, they face a skeptical judiciary.[305] State actors are likely to reach for more than they can grasp through formal modes of enforcement.

Put simply, America worries about governmental restrictions on speech. The country has a deeply-held normative conviction that speech regulation ought to pass through the crucible of democratic processes and judicial review. We should be suspicious when government seeks to obtain results from private bargains that would be uncertain at best through formal public processes, from parties structurally inclined to concede the point.

2. Process and Information Restrictions

The second approach to assessing legitimacy is to examine the process by which the restriction is generated. In prior works, I elucidated[306] and applied[307] a methodology for normative judgments of online censorship, focusing on whether the decisions to censor are open, transparent, narrowly targeted, and accountable.[308] This formula can be used to evaluate informal government pressures as well as formal rules; indeed, many systems of online control depend upon a blend of public and private efforts.[309] This Article now employs the process-based framework to compare informal methods of altering platforms' content decisions to more formal mechanisms.

ALB. L. REV. 409 (2013) (discussing recent cases).

305. *See supra* note 70 and accompanying text; PROTECT IP Act of 2011, S. 968, 112th Cong. (2011); Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011).

306. *See* Bambauer, *Cybersieves*, *supra* note 258.

307. *See generally* Bambauer, *Orwell's Armchair*, *supra* note 58; Derek E. Bambauer, *Filtering in Oz: Australia's Foray into Internet Censorship*, 31 U. PA. J. INT'L L. 493 (2009).

308. *See* Bambauer, *Cybersieves*, *supra* note 258, at 390–409.

309. *See, e.g.*, *China*, OPENNET INITIATIVE (Aug. 9, 2012), https://access.opennet.net/wp-content/uploads/2011/12/accesscontested-china.pdf; Duncan Geere, *Cameron's Proposed Filters Extend to More than Just Porn*, WIRED (July 27, 2013); http://www.wired.co.uk/news/archive/2013-07/27/pornwall; Laurie Penny, *David Cameron's Internet Porn Filter Is the Start of Censorship Creep*, GUARDIAN (Jan. 3, 2014), http://www.theguardian.com/commentisfree/2014/jan/03/david-cameron-internet-porn-filter-censorship-creep.

Openness varies: the government discloses some jawboning publicly, but pressures often begin (and sometimes remain) behind closed doors.[310] The concern regarding openness is strategic behavior—regulators will tend to keep their efforts quiet when it suits their interests, and to trumpet them when they wish to add public pressure to their schemes. At minimum, jawboning is inherently less open than formal rulemaking through legislation, adjudication, or administrative procedure.[311] In addition, regulators disclose informal efforts intermittently at best. Relative to more formal mechanisms, jawboning fares poorly on the openness criterion.

The transparency analysis is similar to that for openness. Transparency measures whether regulators are clear about what content is proscribed, in addition to whether content restrictions should be put in place (which is measured by openness).[312] While the level of transparency will vary with the specifics of the governmental effort, there is no reason to think that requests to remove, for example, material that infringes copyright or that constitutes child pornography will be less specific and comprehensible to platforms than formal regulations that so specify.[313] Generally, more formal means are more transparent, because informal statements may be ephemeral.[314] Here, though, the relationship between regulator and regulated diminishes that concern. Where there is uncertainty, platforms can likely seek informal assistance from regulators, who are likely to clarify areas of uncertainty; this method may be superior from a cost perspective. Thus, for transparency, jawboning does not seem worse than formal regulation, and it may have some advantages.

---

310. *Compare supra* Part I.B (describing open jawboning of Backpage.com), *with supra* Part I.D (describing closed negotiations over Six Strikes).

311. *Cf.* Bambauer, *Cybersieves*, *supra* note 258, at 390 ("[C]ensorship that is clearly disclosed and carefully explained is more likely to be legitimate, [while] censorship that is covert, or that rests on flimsy pretexts, is less acceptable.").

312. *See id.* at 393.

313. *See, e.g.*, 17 U.S.C. § 512(c) (2012); 18 U.S.C. § 2258 (2012).

314. *Cf.* Bambauer, *Cybersieves*, *supra* note 258, at 394–95 ("States can disclose what material they block either formally, such as through codification in press regulations, or informally, such as in statements by government officials. Formal criteria are more transparent; citizens have greater access to documented rules than to oral utterances." (footnotes omitted)).

Jawboning is unlikely to target proscribed content narrowly.[315] In theory, informal pressures could carefully concentrate only upon unlawful material. If they aim only at content designated as illegal through legitimate procedures, these efforts are less likely to be problematic. While there is the problem of underinclusive enforcement, the government can choose to start by tackling part of the issue.[316] Regulators may be less likely to use informal means to pursue unlawful content, in part because they generally do not need to. However, governments may decide to apply pressure to platforms even when the content is not unlawful as to the firms (rather than their users).[317] Jawboning is thus wide in practice, even if narrow in theory.

The largest legitimacy challenge for jawboning is accountability.[318] In the United States, all government officials are ultimately accountable to the polity, though varying levels of effort are required to remove them.[319] The accountability analysis, though, is more subtle than merely probing for whether constituents vote for their officials.[320] Citizens' power

315. *See id.* at 397–99 (explaining that filtering may be overinclusive, underinclusive, or a combination of both, depending on the content).

316. There remain salient constitutional limits on partial enforcement. For example, the government may not target only obscene speech produced by Democrats. *See* R.A.V. v. City of St. Paul, 505 U.S. 377, 382–89 (1992). The Supreme Court, in *R.A.V.*, rejected the notion that its approach banned underinclusiveness, rather than content discrimination. *Id.* at 387. Perhaps the more accurate description is that the Court limits the reasons why content regulation, even of expression that the state may proscribe, can be underinclusive.

317. *See generally* Jones v. Dirty World Entm't Recordings L.L.C., 755 F.3d 398, 407–08 (6th Cir. 2014); UMG Recordings, Inc. v. Shelter Capital Partners L.L.C., 718 F.3d 1006, 1011–14 (9th Cir. 2013); Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 26–28 (2d Cir. 2012); Green v. Am. Online (AOL), 318 F.3d 465, 470–71 (3d Cir. 2003).

318. *See* Bambauer, *Cybersieves*, *supra* note 258, at 400–01.

319. For example, a sitting President may hold office only for a maximum of ten years (if re-elected twice, and initially serving half of the prior President's term), whereas Article III federal judges hold their positions for life (technically, during "good Behavior"). U.S. CONST. amend. XXII, § 1, cl. 1 ("No person shall be elected to the office of the President more than twice, and no person who has held the office of President, or acted as President, for more than two years of a term to which some other person was elected President shall be elected to the office of the President more than once."); U.S. CONST. art. III, § 1, cl. 2 ("Judges, both of the supreme and inferior Courts, shall hold their Offices during good Behavior . . . .").

320. *See* Bambauer, *Cybersieves*, *supra* note 258, at 402–04 (describing problems of accountability in countries lacking citizen participation and accountability failures in democracies).

to elect their government may be transitory[321] or illusory[322]; in a federal system, a regulator in one state may take action with spillover effects into other states, where residents cannot force the regulator to feel their disapprobation.[323] The accountability analysis incorporates four parts: first, democratic participation; second, specification of authority; third, opportunity to challenge; and fourth, countermajoritarian constraints.[324] In the U.S., jawboning passes muster on the first—state actors are elected, or report to those who have been—but falters on the others. The second piece of the accountability test measures whether the state's legal authority to demand removal or alteration of content is clearly delineated.[325] Express selection of content still may not be sufficiently precise, such as with statutes prohibiting online services from making indecent material available to minors.[326] Overly broad proscriptions can enable regulators to pursue violators arbitrarily or as pretext for other motives.[327]

The opportunity to challenge is, formally, likely to be present in nearly all contexts.[328] However, the challenge itself comes at a cost. At minimum, the platform contesting informal efforts has to invest time and resources.[329] Lawyers are not cheap. Further, the switch to formal mechanisms, such as a

321. *See id.* at 402 (using the example of Thailand, where coups have repeatedly displaced elected governments).

322. *See id.* at 402–03 (noting that Russia and Zimbabwe have the procedural trappings but not the substance of democratic participation); FREEDOM HOUSE, FREEDOM IN THE WORLD 2014: THE DEMOCRATIC LEADERSHIP GAP 21–22 (2014), https://freedomhouse.org/sites/default/files/FIW%202014%20Scores%20-%20Countries%20and%20Territories.pdf (designating Russia and Zimbabwe as "Not Free").

323. *See, e.g.*, Bambauer, *Cybersieves*, *supra* note 258, at 403 (describing how New York's Attorney General pressured ISPs into dropping Usenet service for all of the providers' customers, not just those in New York).

324. *Id.* at 400–01.

325. *Id.* at 404–06.

326. *See, e.g.*, Reno v. Am. Civ. Liberties Union, 521 U.S. 844, 859, 874–75 (1997) (invalidating 47 U.S.C. § 223(a), which created criminal penalties for allowing telecommunications facility to be used to transmit indecent material).

327. *See id.* at 871–72. *See generally* Bambauer, *Cybersieves*, *supra* note 258, at 405 (noting Singapore's use of broad definitions of prohibited content to selectively ban popular gay and lesbian sites).

328. *See* Kreimer, *supra* note 57, at 31–32 ("[E]fforts to generate proxy censorship by targeting intermediaries are less likely to be challenged in court than censorship efforts directed at speakers or listeners, and are therefore more likely to be consciously manipulated to suppress protected speech.").

329. *See id.*

lawsuit, is virtually certain to draw publicity. As Tim Wu notes, sometimes publicity itself is punishment.[330] Going public can draw in other parties, either those with affected interests or those acting opportunistically.[331] For the regulator, part of the benefit of jawboning is that it transfers much of the costs of enforcement to the target entity; rather than engaging in expensive rulemaking or adjudication, the government can persuade or threaten, and force the target to seek recourse through more costly channels.[332] Companies do occasionally stand up to the regulator on principle. For example, Yahoo! challenged a gag order contained in a subpoena for information on one of its users in federal court.[333] The government sought to keep Yahoo! from informing the user indefinitely, rather than for the usual 60- or 90-day limit.[334] The Internet firm's successful effort meant that it could tell the user they were under investigation—valuable to that person, but only minimally so to the company.[335] While Yahoo! likely earned reputational benefit in some circles, it is difficult to believe the bump in prestige would offset the costs.[336] Again, platforms are unlikely to internalize the benefits of a challenge, in the same way that some of the costs of regulation fall upon users rather than the firm. Thus, even though regulated parties do possess the power to challenge jawboning, they will often be deterred from doing so.[337]

---

330. Wu, *supra* note 49, at 1856.

331. For example, Google's challenge to Mississippi Attorney General Jim Hood's subpoena drew a range of amicus briefs from groups on both sides of the issue, including the Electronic Frontier Foundation, Digital Citizens Alliance, and the International AntiCounterfeiting Coalition. Ernesto, *Google Chrome Dragged into Internet Censorship Fight*, TORRENTFREAK (Feb. 5, 2015), http://torrentfreak.com/google-chrome-dragged-internet-censorship-fight-150205.

332. *See* Memorandum of Law, *supra* note 18, at 8–13 (describing the Attorney General's threats which caused Google Inc. to seek recourse through the courts); Mullin, *supra* note 10; Sales, *supra* note 27.

333. Order Denying Motion Pursuant to 18 U.S.C. § 2705(b), *In re* Grand Jury Subpoena for: [Redacted]@yahoo.com, No. 5:15-xr-90096-PSG (N.D. Cal. Feb. 5, 2015).

334. *Id.* at *1.

335. *See* Caroline Simson, *US Bid for Unending Yahoo Gag Order Rejected by Judge*, LAW360 (Feb. 9, 2015), http://www.law360.com/articles/619364/us-bid-for-unending-yahoo-gag-order-rejected-by-judge (noting decision subject to re-filing by government for shorter period of non-disclosure).

336. *See Google, Yahoo, Facebook and Microsoft Push Back on Surveillance Gag Orders*, RT (May 24, 2014), http://www.rt.com/usa/161192-google-facebook-microsoft-nsa-gag.

337. *See* Noah, *supra* note 53. For example, only two firms have challenged

The last prong in the accountability analysis tests whether there are countermajoritarian constraints on censorship decisions.[338] As with opportunity to challenge, those constraints are formally present via judicial challenge to jawboning, among other options. But the initial interaction lacks direct constraints—regulators are either elected or answer to elected officials. They have few incentives to consider minority viewpoints, so long as those viewpoints are not those of powerful interest groups.[339] Informal enforcement will generally lack countermajoritarian constraints, since there is no neutral arbiter—only the regulator and the regulated. Moreover, procedural hurdles—including doctrines such as standing and ripeness—may limit targets' ability to challenge informal enforcement, thereby obviating the role of courts as a countermajoritarian check.[340]

When comparing more formal modes of enforcement to less formal ones, both the process-based approach and the constitutional structure and values approach manifest a distinct preference for the formal. Formal mechanisms are generally more open and accountable, and better comport with America's structural reluctance to countenance speech restrictions.

III. WHAT IS TO BE DONE?[341]

If jawboning is both illegitimate and sufficiently widespread to warrant remediation, what is to be done? This Part

---

the FTC's efforts to force compliance with their privacy and security norms, even though the settlements that all other firms agree to impose significant monitoring obligations as well as financial penalties. LabMD v. Fed. Trade Comm'n, No. 14-12144 (11th Cir. 2015), http://www.ftc.gov/system/files/documents/cases/d09351labmdappealorder_0.pdf; Fed. Trade Comm'n v. Wyndham Worldwide, No. 13-cv-1887 (ES) (D.N.J. 2014). Only three enforcement actions to date have failed to end in settlement. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 611–12 (2014).

338. Bambauer, *Cybersieves*, *supra* note 258, at 408.

339. *See supra* notes 6–19 (noting that Hollywood content companies are a minority interest group, but that they are not a powerless group).

340. *See* Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334 (2014) (finding case ripe for adjudication); Hollingsworth v. Perry, 133 S. Ct. 2652 (2013) (denying standing). *See generally* Nicholas Quinn Rosencranz, *The Subjects of the Constitution*, 62 STAN. L. REV. 1209 (2010) (discussing ripeness and standing as prerequisites to judicial review).

341. With apologies to Leo Tolstoy. LEO TOLSTOY, WHAT IS TO BE DONE? (English ed. 1887).

reviews first the considerable challenges to cabining jawboning. Then, it explores and evaluates the options to do so.

A. CHALLENGES

Jawboning is difficult to constrain for a variety of reasons. First, government can effectively threaten platforms even when its underlying legal authority is unclear, or its capability to obtain such authority in the future is uncertain. Firms must bear the costs of clarifying the scope of the state's power, either by challenging it or by incurring risk of future, formal enforcement. Even if the state actor lacks authority at present, she could seek it through rulemaking or legislation, leaving the target in an even worse position since the ambiguity would vanish.[342] For the regulated, predicting whether a regulator has the political clout to obtain new authority is risky business.[343] Even efforts likely to fail may force firms to expend resources in lobbying against them, just to be certain of the outcome. In short, the state uses the cost calculus of uncertainty and transactional expenses to push firms to comply.

Second, platforms may lack incentives to try to cabin jawboning.[344] A platform that resists pressure creates, in effect, a public good—clarifying the scope of governmental authority—but it captures only a small fraction of the benefit of that good, leading to underproduction.[345] Firms may also have strategic reasons to favor, even subtly, jawboning.[346] Close relationships with regulators may mean that the informal guidance

342. Network neutrality provides one example. The FCC began by jawboning, and eventually reclassified broadband Internet as subject to common carrier regulation. FCC, FCC ADOPTS STRONG, SUSTAINABLE RULES TO PROTECT THE OPEN INTERNET (Feb. 26, 2015), https://www.fcc.gov/document/fcc-adopts-strong-sustainable-rules-protect-open-internet.

343. For example, network neutrality rules were viewed as unlikely to pass, while SOPA and PROTECT IP appeared to be safe bets to be enacted. *See* Tim Wu, *Why Everyone Was Wrong About Net Neutrality*, NEW YORKER (Feb. 26, 2015), http://www.newyorker.com/business/currency/why-everyone-was-wrong-about-net-neutrality; *see also* Grant Gross, *Lawmakers Seem Intent on Approving SOPA, PIPA*, PCWORLD (Jan. 5, 2012), http://www.pcworld.com/article/247339/lawmakers_seem_intent_on_approving_sopa_pipa.html.

344. *See* Kreimer, *supra* note 57.

345. *See id.* at 31–32.

346. Wu, *supra* note 49, at 1843 ("[B]oth industry and agency may sometimes prefer unenforceable rules and a lack of judicial involvement. . . . The costs of a slow-moving, ossified rulemaking or adjudicatory procedure, with its accompanying uncertainty and litigation costs, fall on both industry and agency.").

needed to comply is more readily available to existing firms than to new market entrants. The sheer opacity of enforcement can helpfully create barriers to entry—and thus competition.

Third, jawboning operates offstage and is hard to detect. Government frequently operates in private—behind closed doors, where countervailing forces and pressures are excluded.[347] A lack of transparency impedes efforts to check jawboning.[348] It may be hard to determine the frequency with which it is employed. The state may credibly threaten greater or additional penalties if the target reveals government pressure.[349] The federal government has not hesitated to employ this type of leverage. For example, when the telecommunications firm Qwest refused the National Security Agency's request to provide phone records without a warrant, the government allegedly withdrew contracts worth hundreds of millions of dollars.[350] Conversely, the government can go public with its concerns with virtually no fear of penalty.[351] Moreover, public enforcers may engage in misdirection. They may lie. Project Goliath supplies a cogent example: Attorney General Hood sought to pressure Google under the guise of concern over trafficking in illegal pharmaceuticals, pornography, and stolen credit cards, when his real rationale was Hollywood's loathing of copyright infringement.[352] His true motivation came to light only when

347. *See* Mark Fenster, *The Opacity of Transparency*, 91 IOWA L. REV. 885, 934 (2006) ("[A]gencies that face avoidable openness requirements may operate in the ways transparency theory anticipates, by disclosing what they must while keeping secret that which is best left undisclosed . . . .").

348. *Cf.* Frederick Schauer, *Transparency in Three Dimensions*, 2011 U. ILL. L. REV. 1339, 1347–48 (discussing transparency as regulation).

349. *See* Order Denying Motion Pursuant to 18 U.S.C. § 2705(b), *In re* Grand Jury Subpoena for: [Redacted]@yahoo.com, No. 5:15-xr-90096-PSG (N.D. Cal. Feb. 5, 2015) (rejecting government's motion to prevent Yahoo! from disclosing grand jury subpoena for indefinite period on First Amendment grounds); Kim Zetter, *"John Doe" Who Fought FBI Spying Freed from Gag Order After 6 Years*, WIRED (Aug. 10, 2010), http://www.wired.com/2010/08/nsl-gag-order-lifted (describing ISP owner who fought gag order regarding National Security Letter, and noting that "the letter's gag order 'was totally clear that they were saying that I couldn't speak to a lawyer'").

350. Ellen Nakashima & Dan Eggen, *Former CEO Says U.S. Punished Phone Firm; Qwest Feared NSA Plan Was Illegal, Filing Says*, WASH. POST, Oct. 13, 2007, at A1.

351. *See* Yochai Benkler, *A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311, 331–33, 338–44 (2011) (describing informal government pressures on Wikileaks).

352. *See* Wingfield & Lipton, *supra* note 14.

the Sony Pictures hack caused a trove of e-mail messages about Project Goliath to emerge.[353] This misdirection lets government optimize its rationale for intervention, even when that rationale is less than the truth.

Fourth, the primary source of checks on the elected branches—judicial intervention—is dramatically limited by doctrine. Targets of jawboning may have trouble proving standing under Article III, since it may be hard to demonstrate sufficient fear of enforcement from informal demands and discussions.[354] Similarly, remedies are challenging—courts may be reluctant to intervene in the operations of their co-equal branches. In particular, judges may be chary of enjoining what appears to be government speech—a category of expression nearly free of constitutional limitations.[355] The boundary between threats and speech is hard enough to divine when dealing with private actors; with government, it is yet more difficult.[356] Targets of jawboning may be trapped in a paradox: facing enough risk of enforcement to prompt action, but not enough to trigger judicial review.[357]

Lastly, there may be risks of second-order jawboning in some cases. For example, Internet firms that do business with

353. *See* Adi Robertson, *Google Condemns Hollywood's Secret Anti-Piracy Program*, VERGE (Dec. 18, 2014), http://www.theverge.com/2014/12/18/7417891/google-condemns-sony-project-goliath.

354. *See* Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2342, 2344 (2014) (allowing "pre-enforcement review under circumstances that render the threatened enforcement sufficiently imminent" and requiring that the conduct be arguably forbidden by the challenged statute).

355. *See* Walker v. Tex. Div., Sons of Confederate Veterans, 135 S. Ct. 2239, 2245 (2015) ("When government speaks, it is not barred by the Free Speech Clause from determining the content of what it says." (citing Pleasant Grove v. Summum, 555 U.S. 460, 467–68 (2009))); Pleasant Grove v. Summum, 555 U.S. 460, 467 (2009) ("The Free Speech Clause restricts government regulation of private speech; it does not regulate government speech."). *But see* Nelson Tebbe, *Government Nonendorsement*, 98 MINN. L. REV. 648, 650 (2013) (arguing "that in fact the Constitution properly imposes a broad principle of government nonendorsement") .

356. *See* Gia Lee, *Persuasion, Transparency, and Government Speech*, 56 HASTINGS L.J. 983, 1005–08 (2005) (explaining that government communications are becoming less transparent because of the developments in technology and society).

357. State courts, of course, are not bound by Article III's limitations and could, consistent with their own constitutional and statutory limits, intervene earlier. For example, the Massachusetts Supreme Judicial Court propounded an advisory opinion on civil unions in response to a request from the state's legislature. *In re* Opinions of the Justices to the Senate, 802 N.E.2d 565 (Mass. 2004).

the government may be motivated to respond to state preferences, or risk seemingly unconnected penalties in contracting. Or, principal-agent divergence may cause problems. A number of top executives at companies such as Google and Twitter have moved between the government and the private sector, particularly in the Obama administration.[358] Others may be motivated to nudge their firms to comply so as to remain viable candidates for government jobs. This possibility requires a signaling mechanism—the target must know about the causal link between lack of compliance and the seemingly unrelated penalty—but repeated interactions over time may provide the necessary clues.

These barriers to resisting jawboning only serve to reinforce the power of the tactic against platforms. Regulators can use threats and other informal enforcement tools to prod recalcitrant Internet firms, knowing that structural factors push towards compliance. The next Section examines options to shift this calculus.

B. PARTIAL REMEDIES

With these challenges in mind, four possibilities bear consideration: changing legal doctrine to alter jawboning, using reputational rewards and sanctions, encouraging transparency, and framing the practice as illegitimate.

358. *See* Cecilia Kang & Juliet Eilperin, *Why Silicon Valley Is the New Revolving Door for Obama Staffers*, WASH. POST (Feb. 28, 2015), http://www.washingtonpost.com/business/economy/as-obama-nears-close-of-his-tenure-commitment-to-silicon-valley-is-clear/2015/02/27/3bee8088-bc8e-11e4-bdfa-b8e8f594e6ee_story.html. For example, Andrew McLaughlin moved from Google to the Obama administration to Digg. *About Andrew*, ANDREW MCLAUGHLIN, http://andrew.mclaughl.in/about-me (last visited Oct. 14, 2015). Former White House Chief Technology Officer Aneesh Chopra started a data analytics firm. Steven Overly, *Aneesh Chopra, the Nation's First Chief Technology Officer, Has Started a New Venture*, WASH. POST (Mar. 23, 2014), http://www.washingtonpost.com/business/capitalbusiness/aneesh-chopra-the-nations-first-chief-technology-officer-has-started-a-new-venture/2014/03/21/51e20d3a-afa4-11e3-9627-c65021d6d572_story.html. David Kappos was nominated to join the Obama administration as head of the U.S. Patent and Trademark Office from IBM. Office of the Press Secretary, *President Obama Announces More Key Administration Posts*, WHITE HOUSE (June 18, 2009), http://www.whitehouse.gov/the_press_office/President-Obama-Announces-More-Key-Administration-Posts-6-18-09.

1. Limits Through Law

One could attempt to limit jawboning through law. This would build on the extant, though scanty, constitutional protections for platforms that might bar at least some jawboning. The unconstitutional conditions doctrine limits the bargains government can strike when it demands the surrender of one constitutional right to obtain a benefit.[359] The doctrine likely constrains informal pressures well at the edges—when the state demands a decision about content without any legal authority to regulate that content.[360] That looks like duress, or a one-sided bargain: government gains a benefit without surrendering anything.[361] With Project Goliath, this analysis is straightforward. The state attorneys general have nothing to trade for Google's compliance with their demands. With data retention, the calculus is harder—it's not at all clear that the government's threat to seek legislation mandating records retention is a nullity.[362] However, in anything but edge cases, the unconstitutional conditions doctrine is an enigma wrapped in a mystery—its boundaries, terms, and justifications are uncertain at

359. *Compare* Agency for Int'l Dev. v. All. for Open Soc'y Int'l, 133 S. Ct. 2321 (2013) (rejecting the condition for international aid funding that required opposition to prostitution), *and* Koontz v. St. Johns River Water Mgmt. Dist., 133 S. Ct. 2586 (2013) (rejecting government demand for an easement and offsetting wetland improvements in exchange for development permit), *with* United States v. Am. Library Ass'n, 539 U.S. 194 (2003) (upholding the requirement that libraries and schools instill filters on Internet-connected computers to obtain government-subsidized broadband access), *and* Regan v. Taxation with Representation of Wash., 461 U.S. 540 (1983) (upholding the requirement that entities refrain from lobbying in order to maintain tax-exempt status).

360. *Cf.* Hamburger, *supra* note 58, at 480 ("[C]onsent is irrelevant for conditions that go beyond the government's power.").

361. *See* Daniel A. Farber, *Another View of the Quagmire: Unconstitutional Conditions and Contract Theory*, 33 FLA. ST. U. L. REV. 913, 943 (2006) ("Judicial review of the qualitative match between the two sides of a bargain has no counterpart in contract law. This suggests that the motivating concerns are quite different than those relating to ordinary markets, such as preventing duress."). *But see* Adam B. Cox & Adam M. Samaha, *Unconstitutional Conditions Questions Everywhere: The Implications of Exit and Sorting for Constitutional Law and Theory*, 5 J. LEGAL ANALYSIS 61, 65 (2013) ("Deal-making is ordinarily a good thing, even if the situation seems like 'a choice between the rock and the whirlpool.'" (quoting Michigan P.U.C. v. Duke, 266 U.S. 570, 593 (1925))).

362. Data retention is already statutorily required in some industries, including the securities industry and health care industry. *See* Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 641–42 (2011).

best and arbitrary at worst.[363] It is not clear when the unconstitutional conditions doctrine is triggered, nor what methodology courts use to resolve cases when it is.[364] This aspect of constitutional law cannot reliably check jawboning.

Other legal options founder on practical considerations. Regulators could simply forbear from employing jawboning, but that disposes of the problem via wishful thinking. Congress could limit the executive's scope of freedom by imposing statutory constraints, as it has done with the Federal Trade Commission (FTC)[365] and Environmental Protection Agency (EPA).[366] This would narrow, but not eliminate, executive branch enforcement. For example, despite the significant limitations on its substantive rulemaking authority, the FTC has effectively become the chief privacy regulator for the U.S., establishing a pattern of settlements that constitute a type of common law for the area.[367] And this possibility assumes that Congress wants to check executive jawboning, which was not

---

363. *See* Bambauer, *Orwell's Armchair*, *supra* note 58, at 917 (arguing that the logic of the unconstitutional conditions doctrine is unclear and that courts engage in guesswork when utilizing the doctrine); Richard A. Epstein, *Unconstitutional Conditions, State Power, and the Limits of Consent*, 102 HARV. L. REV. 4, 11 (1988) ("The [academic literature] sensibly recognizes the essential place that the [unconstitutional conditions] doctrine occupies in modern constitutional law, but it makes far less sense when it attempts to explain how the doctrine arises or what it does."); Hamburger, *supra* note 58, at 487–88 (describing how case law is confusing because courts reach decisions before fully understanding the issue).

364. Cox & Samaha, *supra* note 361, at 67 ("[A]n amusing aspect of the unconstitutional conditions doctrine is that there is no doctrine . . . there is no snappy and established test for analyzing unconstitutional conditions questions.").

365. 15 U.S.C. § 57a (2012) (limiting the FTC's authority to prescribe rules and general statements of policy). Congress moved to limit the FTC's substantive rulemaking authority in 1975 with the Magnuson-Moss Warranty Act, hemming in the agency with a set of baroque procedural requirements. Magnuson-Moss Warranty-Federal Trade Commission Improvement Act, Pub. L. No. 93-637, § 202, 88 Stat. 2183, 2193 (1975).

366. 42 U.S.C. § 7479(3) (2012). The Environmental Protection Agency must consider "energy, environmental, and economic impacts and other costs" when determining what constitutes the best available control technology mandated by the Clean Air Act.

367. *See* Solove & Hartzog, *supra* note 337, at 585–86 (explaining how FTC jurisprudence is the "broadest and most influential regulating force on information privacy" and that companies analyze the settlement agreements to guide their decisions). *But see* Justin Hurwitz, *Data Security and the FTC's UnCommon Law*, IOWA L. REV. (forthcoming 2015) (manuscript at 20) (on file with author) (arguing that the FTC's discretion to select cases it will hear is a "clear departure from the common law").

the case in the data retention debate at least.[368] The executive branch could impose its own internal controls on informal enforcement. For example, the Department of Justice requires that U.S. Attorneys obtain approval from designated senior officials, such as the Associate Attorney General, before entering into bargains allowing pleas of *nolo contendere*.[369] However, the executive is not likely to limit significantly its own enforcement powers and discretion. This option, too, assumes the problem away. Put simply, the political branches find jawboning too easy, attractive, and powerful to impose meaningful internal or interbranch checks on the practice. And, the demands of the modern administrative state make regulators wary of limiting informal enforcement.[370]

2. Reputational Consequences

A second possibility is for private entities such as consumers and civil society groups to generate approbation for platform resistance to jawboning, and disapprobation for acquiescence. They should applaud Google when the firm keeps videos of police brutality on its YouTube site despite government pressure, and decry the search engine when it takes down offensive films based upon it.[371] Increasing the reputational consequences to firms based on their decisions about whether to submit to jawboning seem initially to have the moral calculus backwards—a form of blaming the victim. However, this method constrains government from a different angle. Firms will inevitably vary with how pliant they are in responding to informal

368. *See supra* Part I.D.

369. U.S. DEP'T OF JUSTICE, U.S. ATTORNEYS' MANUAL, APPROVAL REQUIRED FOR CONSENT TO PLEA OF NOLO CONTENDERE § 9-16.010 (2008), http://www.justice.gov/usam/usam-9-16000-pleas-federal-rule-criminal-procedure-11#9-16.010.

370. *See* Wu, *supra* note 49, at 1842 (contending that threats are useful since the alternatives are ignoring issues or making laws without a sufficient factual record).

371. *Compare* Rebecca J. Rosen, *What To Make of Google's Decision To Block the "Innocence of Muslims" Movie*, ATLANTIC (Sept. 14, 2012), http://www.theatlantic.com/technology/archive/2012/09/what-to-make-of-googles-decision-to-block-the-innocence-of-muslims-movie/262395 (suggesting that pressure from the Obama administration contributed to Google's removal of the film), *with* Rebecca J. Rosen, *Google Refuses To Remove Police-Brutality Videos*, ATLANTIC (Oct. 27, 2011), http://www.theatlantic.com/technology/archive/2011/10/google-refuses-to-remove-police-brutality-videos/247462 (uncovering that Google generally removes content only when receiving court orders declaring content as defamatory).

state pressures. For example, under the administration of President George W. Bush, the National Security Agency sought to obtain American citizens' telephone records from telecommunications companies without a warrant.[372] AT&T, Verizon, and BellSouth readily complied.[373] Qwest refused.[374] Imposing reputational consequences for those decisions would reward Qwest, relative to its competitors, for resisting jawboning to undertake illegal action.

Rewarding or punishing firms for resisting (or acquiescing to) jawboning would have at least two salutary effects. First, it can generate a market-based return—or penalty—that helps platform companies internalize the effects of their decisions. This could shift, though perhaps only partially, the structural incentives that lead intermediaries to comply so readily with informal measures. There is some evidence that this occurs when companies take inadequate precautions in other areas, such as cybersecurity. Researchers have found a small but significant negative effect on the stock price of firms that suffer a data breach.[375] Second, if successful, these efforts can begin to drive industry expectations and norms. Those norms not only have soft power, they may be translated into pecuniary terms if investors such as socially-responsible mutual funds incorporate them into purchasing decisions. Soft power alone should not be discounted. Google's decision to begin its Transparency Reports in 2010—which detail the number of requests such as copyright takedown notices and demands to remove content,[376]—led a number of Internet firms to engage in the same disclosures.[377] A

372. *See* John O'Neil & Eric Lichtblau, *Qwest's Refusal of N.S.A. Query Is Explained*, N.Y. TIMES (May 12, 2006), http://www.nytimes.com/2006/05/12/washington/12cnd-phone.html.

373. *See id.*

374. *See id.* (discovering Qwest concluded that completing the requests for the telephone records without a warrant would violate the privacy requirements of the Telecommunications Act).

375. *See* Edward A. Morse et al., *Market Price Effects of Data Security Breaches*, 20 INFO. SEC. J. GLOBAL PERSP. 263, 271 (2011) (concluding that investors are influenced by data breaches); Alessandro Acquisti et al., Address at the Twenty Seventh International Conference on Information Systems and Workshop on the Economics of Information Security: Is There a Cost to Privacy Breaches? An Event Study (2006), http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf.

376. *See Transparency Report*, GOOGLE, http://www.google.com/transparencyreport (last visited Oct. 14, 2015); *see* Jane R. Bambauer & Derek E. Bambauer, *Vanished*, 18 VA. J.L. & TECH. 137, 140–48 (2013).

377. *See* Ryan Budish, *What Transparency Reports Don't Tell Us*, ATLANTIC

norm of resistance can help ameliorate potential collective action problems with jawboning—but a company considering whether to comply must consider the possibility that if it balks, and competitors acquiesce, it will find itself a target for regulatory scrutiny.

The promise of reputational consequences is uncertain, though, because there are two impediments to implementation. Interested parties have to learn about jawboning attempts to respond to them. At minimum, disclosure is not routine: the Obama administration disclosed information about its pressures on ISPs to adopt Six Strikes only in response to a Freedom of Information Act (FoIA) lawsuit, and details about Project Goliath came to light as a result of the Sony hack (allegedly related to the movie "The Interview"). Neither movie studio cybersecurity breaches nor FoIA suits are the norm. Reputational sanctions can still operate in an environment of episodic disclosure, but they are likely less effective.[378]

In addition, the mechanisms for imposing consequences are not perfectly understood. Stock divestment, social media campaigns, protests, critical media coverage, ratings by civil society groups—all of these contribute, but not in a consistent or predictable fashion. And effects might be short-lived. For many data breaches, stock prices recover completely after only a month.[379] Using reputational penalties and rewards to counterbalance jawboning is an appealing concept, but one difficult to translate precisely into practice.

(Dec. 19, 2013) http://www.theatlantic.com/technology/archive/2013/12/what-transparency-reports-dont-tell-us/282529 (noting that numerous companies began reporting requests in hopes to gain customer trust); *Who Has Your Back?*, ELECTRONIC FRONTIER FOUND., [hereinafter E.F.F.] https://www.eff.org/who-has-your-back-2014 (last visited Oct. 14, 2015) (listing firms and disclosures).

378. *Cf.* Jay J. Janney & Steve Gove, *Reputation and Corporate Social Responsibility Aberrations, Trends, and Hypocrisy: Reactions to Firm Choices in the Stock Option Backdating Scandal*, 48 J. MGMT. STUD. 1562, 1562 (2011) (finding that firms with enhanced reputations for Corporate Social Responsibility are protected from scandal revelations but are more harshly sanctioned).

379. *See* Eric Chemi, *Investors Couldn't Care Less About Data Breaches*, BLOOMBERG BUS. (May 23, 2014), http://www.bloomberg.com/bw/articles/2014-05-23/why-investors-just-dont-care-about-data-breaches (describing how TJMaxx stock recovered a few months after its data breach, JPMorgan Chase stock recovered two weeks after its data breach and Adobe Systems stock did not decrease after its data breach); Sebastien Gay, Strategic News Bundling and Privacy Breach Disclosures 2 (June 25, 2015) (unpublished manuscript) (on file with author) (explaining that Anthem stock was unaffected after one of the largest privacy breaches in history).

3. Transparency Encouragement

Encouraging Internet firms to be transparent—even imperfectly so—about jawboning efforts can usefully serve as a disinfectant against those measures.[380] There are both internal and external mechanisms for transparency. Internal measures rely upon platforms' cooperation, but Internet firms have been increasingly willing to disclose previously-concealed government enforcement efforts. The Electronic Frontier Foundation listed twenty-six online firms that published transparency reports in 2014[381]—up from one, Google, four years earlier.[382] Internet companies such as Google negotiated with the federal government to report aggregate data about the number of National Security Letters (NSL)[383] that the firms receive on an annual basis.[384]

Similarly, some companies, concerned that they may be legally barred from revealing whether they have received a specific warrant for user data, have begun to employ "warrant canaries."[385] A warrant canary is an inverse signal: it reports that the target platform has *not* received a warrant, subpoena, or NSL.[386] When the canary disappears, users know the firm has

380. Justice Louis Brandeis famously stated that "[s]unlight is said to be the best of disinfectants; electric light the most efficient policeman." *Justice Louis D. Brandeis*, LOUIS D. BRANDEIS LEGACY FUND FOR SOC. JUST., http://www.brandeis.edu/legacyfund/bio.html (last visited Oct. 14, 2015).

381. E.F.F., *supra* note 377.

382. *See* Budish, *supra* note 377.

383. *See* 18 U.S.C. § 2709 (2012). S*ee generally* Doe v. Ashcroft, 334 F. Supp. 2d 471, 478–80 (S.D.N.Y. 2004) (describing Section 2709 and the ability for firms to converse with the government to decide what is necessary to disclose), *vacated and remanded sub nom.* Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006).

384. *See* Letter from James M. Cole, Deputy Attorney General, to Colin Stretch, Esquire, Facebook Corporate Officer, et al. (Jan. 27, 2014), http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf (describing Department of Justice requirements for transparency reporting); *see* Danielle Walker, *Tech Companies, Media Join Twitter's Fight To Divulge NSL Info*, SC MAGAZINE (Feb. 18, 2015), http://www.scmagazine.com/eff-representing-internet-co-telecom-fighting-to-reveal-details-of-nsls/article/398949 (describing Twitter lawsuit to enable firm to disclose additional details about NSLs received).

385. *See* Rebecca Wexler, *Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders*, 124 YALE L.J. F. 158, 159 (2014), http://www.yalelawjournal.org/forum/warrant-canaries-and-disclosure-by-design; CANARY WATCH, https://www.canarywatch.org (last updated Oct. 13, 2015).

386. *See* Wexler, *supra* note 385.

received at least one demand for information.[387] Apple, for example, includes this language in its 2013 Transparency Report: "Apple has never received an order under Section 215 of the USA Patriot Act."[388] In its next Report, that language disappeared, replaced by this notice: "To date, Apple has not received any orders for bulk data," likely indicating that the company has received a more focused demand.[389] Other companies with warrant canaries include SpiderOak, Tumblr, Pinterest, VikingVPN, and Wickr.[390] While transparency reports provide more fine-grained detail than warrant canaries—they indicate both what demands were made and how the platform responded—both types of voluntary disclosures provide a model for how firms could increase transparency regarding jawboning.[391]

It is also possible to have external transparency measures that do not depend upon firms' cooperation. More extreme examples include the Sony Pictures hack and Edward Snowden's disclosures. Guardians of Peace, the group that claimed responsibility for hacking Sony, released a huge volume of internal company documents that revealed not only creative tensions over the movie "The Interview," but also the inner workings of Project Goliath and other private information.[392] Snowden's release of classified NSA documents showed that

---

387. *Id.* at 169.

388. *See* Jeff John Roberts, *Apple's "Warrant Canary" Disappears, Suggesting New Patriot Act Demands*, GIGAOM (Sept. 18, 2014), https://gigaom.com/2014/09/18/apples-warrant-canary-disappears-suggesting-new-patriot-act-demands.

389. *Id. But see* Iain Thomson, *Apple's Warrant Canary Riddle: Cock-up, Conspiracy, or Anti-Google Point-Scoring*, REGISTER (Sept. 20, 2014), http://www.theregister.co.uk/2014/09/20/apples_warrant_canary_is_either_cockup_conspiracy_or_the_antigoogle_selling_point.

390. *See* Jennifer DeTrani, *Wickr Transparency Report (Download)*, WICKR (Oct. 14, 2014), https://wickr.com/category/transparency-report; Greg Kumparak, *SpiderOak Implements a Warrant Canary*, TECHCRUNCH (Aug. 14, 2014), http://techcrunch.com/2014/08/14/spideroak-implements-a-warrant-canary; Derek Zimmer, *The VikingVPN Warrant Canary Is Alive!*, VIKINGVPN (Dec. 9, 2013), https://vikingvpn.com/blogs/transparency/the-vikingvpn-warrant-canary-is-live.

391. *See, e.g.*, *Government Requests To Remove Content*, GOOGLE, http://www.google.com/transparencyreport/removals/government (last visited Oct. 14, 2015) (displaying graph of increasing government requests to Google to remove content between 2010 and 2014). *See generally* Bambauer & Bambauer, *supra* note 376.

392. *See* Russell Brandom, *Everything You Need To Know About the Sony Hacks*, VERGE (Dec. 18, 2014), http://www.theverge.com/2014/12/18/7415735/everything-you-need-to-know-about-the-sony-hacks/in (discussing the emails revealing infighting over pre-production of the movie and anti-piracy efforts).

Microsoft voluntarily aided the NSA in decrypting information sent via the company's Skype, Hotmail, and Outlook Web chat services.[393] Less glamorously, Comcast user Robb Topolski was able to verify that his ISP was not complying with the FCC's jawboning over net neutrality: by running a packet sniffer, he confirmed that Comcast was throttling BitTorrent.[394] Similarly, users could monitor Google's search results—if sites known to infringe copyrighted materials suddenly vanished, they could infer that the company had decided to comply with pressures from state or federal government officials.[395] At a more abstract level, civil society groups could encourage transparency by tabulating and rating the measures firms take to reveal measures such as jawboning.[396]

Whether internal or external, transparency measures are valuable to constraining jawboning. Users, consumers, and civil society organizations should encourage transparency by firms, both as a virtue in itself and as an input into other mechanisms for checking the practice.

4. Normative Labeling

The last possibility is entirely suasive; definitively delineating jawboning as illegitimate can decrease its use. This option provides platforms with rhetorical cover—calling out the

---

393. *See Microsoft Helped the NSA Bypass Encryption, New Snowden Leak Reveals*, RT (July 12, 2013), http://rt.com/usa/microsoft-nsa-snowden-leak-971; Ryan W. Neal, *Snowden Reveals Microsoft PRISM Cooperation: Helped NSA Decrypt Emails, Chats, Skype Conversations*, INT'L BUS. TIMES (July 11, 2013), http://www.ibtimes.com/snowden-reveals-microsoft-prism-cooperation-helped-nsa-decrypt-emails-chats-skype-conversations.

394. *See* Eckersley et al., *supra* note 204.

395. For example, Google began removing sites containing certain personal information under the European Union's "right to be forgotten" ruling. Sam Schechner, *Google Starts Removing Search Results Under Europe's "Right To Be Forgotten,"* WALL ST. J. (June 26, 2014), http://www.wsj.com/articles/google-starts-removing-search-results-under-europes-right-to-be-forgotten-1403774023; *see* Jeffrey Toobin, *The Solace of Oblivion*, NEW YORKER (Sept. 29, 2014), http://www.newyorker.com/magazine/2014/09/29/solace-oblivion. One developer, Afiq Tariq, began a project that tracks every site removed. *About Us*, HIDDEN FROM GOOGLE, http://hiddenfromgoogle.afaqtariq.com/ #aboutus (last visited Oct. 14, 2015) (including thirty censored links affected by the "Right to be Forgotten"); *see* Charlie Osborne, *"Hidden from Google" Tracks Sites Removed from Internet Searches*, CNET NEWS (July 16, 2014), http://www.cnet.com/news/hidden-from-google-tracks-sites-removed-from-internet-searches (describing the website Afiq Tariq created).

396. *See, e.g.*, E.F.F., *supra* note 377; Bambauer, *Cybersieves*, *supra* note 258, at 418–40.

government as "jawboning" has the same effect as accusing the government of "censorship." Painting government efforts as unlawful or simply normatively wrong can have considerable power. Attorney General Hood backed off his efforts to pressure Google once his jawboning came to light. Labeling sets the terms of the debate. It leverages framing by forcing the government to explain why it is not engaging in illegitimate behavior, rather than a legitimate practice.

Framing's power was first documented by cognitive psychologists,[397] and entered popular discourse in the U.S. after politicians latched onto work by cognitive linguist George Lakoff.[398] The concept is that how an idea is described—in particular, the metaphors used—is critical to whether people favor it.[399] Language matters: consumers much prefer the kiwi to the Chinese gooseberry, though they are precisely the same fruit.[400] In the Internet space, examples of framing are legion. Views of Edward Snowden, for example, depend on whether one uses the label "whistleblower" or "traitor"[401]—whether he is a patriot or a terrorist.[402]

The most cogent example for platforms and jawboning was the debate over the Stop Online Piracy and PROTECT IP Acts. At a technical level, arguments over the bills involved questions such as whether the proposed measures would undermine

397. *See* Daniel Kahneman & Amos Tversky, *Prospect Theory: An Analysis of Decision Under Risk*, 47 ECONOMETRICA 263, 287 (1979); Amos Tversky & Daniel Kahneman, *The Framing of Decisions and the Psychology of Choice*, 211 SCIENCE 453, 458 (1981).

398. GEORGE LAKOFF, DON'T THINK OF AN ELEPHANT! KNOW YOUR VALUES AND FRAME THE DEBATE (2004); *see* Matt Bai, *The Framing Wars*, N.Y. TIMES (July 17, 2005), http://www.nytimes.com/2005/07/17/magazine/17DEMOCRATS.html.

399. *See* Bai, *supra* note 398.

400. *See Chinese Gooseberry Becomes Kiwifruit*, NEW ZEALAND HISTORY, http://www.nzhistory.net.nz/the-chinese-gooseberry-becomes-the-kiwifruit (last updated May 29, 2015). Ditto dried plums, which were originally called "prunes." *See* Lisa Zwirn, *The Fruit Formerly Known as Prune Gets a Name Change and a Makeover*, BOS. GLOBE, Oct. 10, 2001, at E3 (explaining that prune producers believed the name change would increase prune sales).

401. *See* Tal Kopan, *Poll: Edward Snowden Still a "Whistleblower*," POLITICO (Aug. 1, 2013), http://www.politico.com/story/2013/08/edward-snowden-nsa-leak-poll-95054.html (finding that 55% of Americans surveyed believed Snowden to be a whistleblower).

402. *See* Sarah Dutton et al., *Poll: Most Think Edward Snowden Should Stand Trial in U.S.*, CBS NEWS (Jan. 22, 2014), http://www.cbsnews.com/news/poll-most-think-edward-snowden-should-stand-trial-in-us.

security of the Domain Name System.[403] At a semantic level, the question was one of framing: would the bills be seen as preventing piracy, or promoting censorship? Both sides employed metaphors that could be outcome-determinative. Who could defend pirating American intellectual property, or suppressing free speech? And both had semantically-loaded terms at their disposal: piracy or censorship. Indeed, the metaphors were embedded in the titles of the bills: piracy (SOPA), and theft of intellectual property (PROTECT IP). Advocates struck the same notes repeatedly in the political discourse. The president of the U.S. Chamber of Commerce stated, "[w]ebsites that blatantly steal the creativity and innovation of American industries violate a fundamental right to property."[404] A Disney Research associate characterized the bills as about "protecting intellectual property," arguing that "[i]f blocking unauthorized access to a work of art that is available ubiquitously through legal channels is censorship, then we need a new definition of censorship."[405] And Senator Patrick Leahy, sponsor of PROTECT IP, commented, "Protecting foreign criminals from liability rather than protecting American copyright holders and intellectual property developers is irresponsible, will cost American jobs, and is just wrong."[406]

By contrast, supporters such as Google chairman Eric Schmidt characterized the bills as "draconian . . . [since they] would require [ISPs] to remove URLs from the web, which is also known as censorship last time I checked."[407] Tumblr argued that the legislation would "establish[] a censorship system us-

403. *See Analysis of SOPA's Impact on DNS and DNSSEC*, ACM U.S. PUBLIC POLICY COUNCIL, http://usacm.acm.org/images/documents/DNSD NSSEC.pdf (last visited Oct. 14, 2015); Letter from Dr. Leonard M. Napolitano, Jr., to Rep. Zoe Lufgren, (Nov. 16, 2011), http://www.scribd.com/doc/73106069/Napolitano-Response-Rep-Lofgren-11-16-11-c.

404. Michail Vafeiadis, *Five Major SOPA Supporters*, CHRISTIAN SCI. MONITOR (Jan. 19, 2012), http://www.csmonitor.com/USA/Elections/2012/0119/Five-major-SOPA-supporters/U.S-Chamber-of-Commerce (quoting Thomas J. Donahue).

405. Anthony Accardo, *Is Copyright Enforcement Censorship?*, HARV. BUS. REV. (Sept. 23, 2011), https://hbr.org/2011/09/is-copyright-enforcement-censo.

406. Sen. Patrick Leahy, *Comment of Senator Patrick Leahy on the PROTECT IP Act*, PATRICK LEAHY (Jan. 17, 2012), http://www.leahy.senate.gov/press/comment-of-senator-patrick-leahy-on-the-protect-ip-act.

407. Michael Sheridan, *SOPA (Stop Internet Piracy Act) Is "Internet Censorship," Says Google & Twitter & Facebook*, N.Y. DAILY NEWS (Nov. 17, 2011), http://www.nydailynews.com/news/national/sopa-internet-censorship-google-twitter-facebook-article-1.979020.

ing the same domain blacklisting technologies pioneered by China and Iran."[408] And Wikipedia co-founder Jimmy Wales described the bills as "outrageous . . . just not acceptable under the First Amendment."[409] SOPA and PROTECT IP lost in part because the censorship frame won.[410] Protecting intellectual property was too indirectly connected with blocking Web sites to gain sway, and safeguarding free speech by preventing censorship is deeply rooted in American mores and constitutional history.

The goal of the normative labeling approach is to make jawboning viscerally undesirable—to conjure the same intellectual and emotional reactions that the term "censorship" arouses. It seeks to make jawboning not only a description of a type of government enforcement, but also an inherent condemnation of the practice. Put simply, saying that an official engaged in jawboning ought to unsettle and offend that person. This plainly involves a change that will require effort. Jawboning is largely a neutral term at present. Wikipedia considers the word synonymous with "moral suasion,"[411] and in business, it routinely connotes an "attempt to persuade others to act in a certain way by using the influence or pressure of a high office."[412] Thus, jawboning does not currently carry the cognitive payload needed to implement this proposal.

But, there is hope—hackers have pointed the way. Originally, the term "hacker" was semantically neutral. It denoted someone with technical skill and curiosity, who enjoyed tinkering, especially with computers.[413] Over time, though, as some of

408. Matt Peckham, *SOPA Won't Stop Online Piracy, Would Censor Everyone Else*, TIME (Nov. 17, 2011), http://techland.time.com/2011/11/17/sopa-wont-stop-online-piracy-would-censor-everyone-else.

409. Amy Goodman & Juan González, *SOPA: Anti-Piracy or Censorship? Wikipedia's Jimmy Wales vs. Copyright Alliance's Sandra Aistars*, DEMOCRACY NOW! (Jan. 19, 2012) (quoting Jimmy Wales), http://www.democracynow.org/2012/1/19/sopa_anti_piracy_or_censorship_wikipedias.

410. *See* Lemley et al., *supra* note 5.

411. *Jawboning*, WIKIPEDIA, http://en.wikipedia.org/wiki/Jawboning (last visited Oct. 14, 2015).

412. *Jawboning*, ALLBUSINESS http://www.allbusiness.com/barrons_dictionary/dictionary-jawboning-4943007-1.html (last visited Oct. 14, 2015). *But see* Thomas G. Donlan, *The Cudgel of Samson: How the Government Once Used "Jawboning" To Fight Inflation*, BARRON'S (Mar. 24, 2008), http://www.barrons.com/articles/SB120614228496656237 (describing "jawboning" as the "government wagging a finger at business and labor to act with restraint, while government acts without restraint" which was ineffective).

413. *See* Ben Yagoda, *A Short History of "Hack,"* NEW YORKER (Mar. 6,

those clever tinkerers put their skills to socially harmful purposes, popular usage of the term embedded a connotation of destructiveness and malice.[414] The technical community prefers the term "cracker" for this purpose, or to distinguish between white hat and black hat hackers, but their distinctions have come to no avail in the wider discourse.[415] The evolution of "hacker" serves as a model for how we should use "jawboning."

There are likely three keys to instantiating this approach. First, proponents of the idea should use the term to describe only illegitimate informal enforcement—and, especially, egregious instances of it. Second, partisans should be attuned to the media's need for shorthand metaphors.[416] This need is more potent than ever with hashtags and 140-character limits for Tweets. Lastly, it helps that there is no group that is particularly invested in maintaining the current semiotic value of the word. As with creating reputational consequences, there is no single or predictable formula for shifting the meaning of jawboning. But the Internet ecosystem of blogs, Twitter, Facebook, and Snapchat means that memes spread quickly. And, the change is likely to appeal to political groupings at either end of the American political spectrum: liberals concerned about the tight relationship between corporations and government, and libertarians worried about overweening state regulation.

The final step for this proposal takes place both during and after the semiotic shift: the term "jawboning" can be used as a weapon. Describing an informal government effort as jawboning will be implicitly to label it as extortion, or blackmail. This can both drive public perception of the move and, if the government takes issue with the characterization, further reinforce the term's new meaning. Americans tend to be inherently skeptical of government, both as a structural matter (given the Constitution's limits on state power) and as a descriptive one (public trust in government has fallen dramatically since the Watergate scandal).[417] As with censorship, deploying the term

---

2014), http://www.newyorker.com/tech/elements/a-short-history-of-hack.

414. *See* Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1098–99 (2011).

415. *See* Chad Perrin, *Hacker vs. Cracker*, TECHREPUBLIC (Apr. 17, 2009, 6:20 AM), http://www.techrepublic.com/blog/it-security/hacker-vs-cracker.

416. *See generally* Jon M. Garon, *Mortgaging the Meme: Financing and Managing Disruptive Innovation*, 10 NW. J. TECH. & INTELL. PROP. 441, 463–67 (2012).

417. *See Public Trust in Government: 1958–2014*, PEW RESEARCH CENTER

jawboning as deprecation can be a potent means for limiting the practice.

CONCLUSION

This Article concludes with observations about how the Article's anti-jawboning position might extend beyond the First Amendment doctrinally, and apply to new situations theoretically.

A. EXTENDING DOCTRINALLY

The skepticism of jawboning defended in this Article is likely generalizable.[418] Free speech concerns, such as pressures on Internet platforms, are a particularly robust test case for the Article's claims: given constitutional and normative constraints on government restrictions on expression, if the core anti-jawboning claims fail here, they likely fail everywhere. While evaluating jawboning in different contexts must be left to future work, this Article suggests briefly that there are other areas where suspicion of the practice is likely to be sustained.

One promising candidate is guns.[419] The Second Amendment, particularly as shaped by the Roberts Court, operates as a potent barrier to governments' regulation of firearms. Bans on home ownership of firearms,[420] retail sales in urban areas,[421]

(Nov. 13, 2014), http://www.people-press.org/2014/11/13/public-trust-in-government (reflecting a general decline in public trust in government beginning in the mid-1970s).

418. The critique of jawboning may have particular salience for rapidly changing or developing technologies beyond the Internet. *See, e.g.*, Maxwell Mensinger, Note, *Remodeling "Model Aircraft": Why Restrictive Language that Grounded the Unmanned Industry Should Cease To Govern It*, 100 MINN. L. REV. 405, 420–39 (2015).

419. *See generally* Sanford Levinson, *The Embarrassing Second Amendment*, 99 YALE L.J. 637 (1989); L.A. Powe, Jr., *Guns, Words, and Constitutional Interpretation*, 38 WM. & MARY L. REV. 1311 (1997); *Attorney General Patrick Morrisey Leads 21 States in Amicus Brief Supporting Citizens' Second Amendment Right to Own Guns*, OFFICE OF THE WEST VIRGINIA ATTORNEY GENERAL (Nov. 18, 2014) http://ago.wv.gov/pressroom/2014/Pages/Attorney-General-Patrick-Morrisey-Leads-21-States-In-Amicus-Brief-Supporting-Citizens'-Second-Amendment-Right-To-Own-Guns.aspx ("[Maryland's] broad categorical ban is no different than trying to impose a content-based ban on speech."). *But see* Gregory P. Magarian, *Speaking Truth To Firepower: How the First Amendment Destabilizes the Second*, 91 TEX. L. REV. 49, 53–59 (2012) (arguing that the differences between First and Second Amendment rights will inhibit judicial protection of gun ownership).

420. *See* District of Columbia v. Heller, 554 U.S. 570 (2008).

421. *See* Ill. Ass'n of Firearms Dealers v. City of Chicago, 961 F. Supp. 2d

public carry,[422] and handgun possession[423] have been struck down in recent years, and the Fourteenth Amendment[424] has provided a vehicle for challenging state and local regulations in addition to federal ones. Like the First Amendment, the Second is not an absolute right, but both provide strong individual entitlements (to speak, or to possess and carry firearms) and the government must offer strong justification before it can invade them.[425]

In addition to courts blocking existing firearms regulations, Congress has rejected proposals for additional restrictions at the federal level. In the wake of the massacre of students and teachers at Sandy Hook Elementary School in Newtown, Connecticut, on December 14, 2012, President Obama vowed to seek new federal gun control legislation.[426] Bipartisan legislation to expand background checks for gun buyers failed in the Senate, though, as it was unable to obtain a filibuster-proof sixty votes, winning only 54–46.[427] On the whole, the past several decades have been ones of retrenchment for gun control efforts: restrictions on firearms have been rolled back consistently at both the federal and state levels.[428]

Here, too, courts and the political branches have circumscribed firearm regulation, causing state actors to move increasingly to jawboning to achieve their ends. Consider guns and banking. The Department of Justice launched Operation Choke Point to pressure financial institutions to reduce lending and payment processing services to fraudulent enterprises.[429]

---

928 (N.D. Ill. 2014).

422. *See* Palmer v. District of Columbia, 59 F. Supp. 3d 173 (D.D.C. 2014).

423. *See* McDonald v. City of Chicago, 561 U.S. 742 (2010).

424. *See id.*

425. *See Heller*, 554 U.S. at 634–35 (linking First and Second Amendment constitutional analysis).

426. *See* Alex Altman, *Obama Takes a First Step on Gun Control After Sandy Hook*, TIME (Dec. 19, 2012), http://swampland.time.com/2012/12/19/obama-takes-a-first-step-on-gun-control-after-sandy-hook.

427. *See* Jeff Zeleny et al., *Obama Takes Senate To Task for Failed Gun Control Measure*, ABC NEWS (Apr. 17, 2013), http://abcnews.go.com/Politics/obama-takes-senate-task-failed-gun-control-measure/story?id=18981374.

428. *See* Kristin Goss, *Two Years After Sandy Hook, the Gun Control Movement Has New Energy*, WASH. POST (Dec. 16, 2014), http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/12/16/two-years-after-sandy-hook-the-gun-control-movement-has-new-energy.

429. *See* Jessica Silver-Greenberg, *Justice Department Inquiry Takes Aim at Banks' Business with Payday Lenders*, N.Y. TIMES (Jan. 26, 2014, 9:59 PM), http://dealbook.nytimes.com/2014/01/26/justice-dept-inquiry-takes-aim-at

Cutting off services to dodgy online payday lenders proved popular, drawing an endorsement from the editorial board of the *New York Times*.[430] But the Federal Deposit Insurance Corporation (FDIC), which regulates certain financial institutions and insures deposits at them, went a step further. It circulated to its members a list of high-risk businesses that posed "elevated . . . legal, reputational, and compliance risks" to their institutions.[431] Along with payday lending, the letter targeted "pornography [and] online tobacco or firearms sales."[432] An earlier iteration of the guidance posted by the FDIC to its Web site listed firearms sales and ammunition sales as "merchant categories that have been associated with high-risk activity," along with "Racist Materials," "Drug Paraphernalia," and "Get Rich Products."[433] Gun dealers were plainly in the FDIC's sights.

Unsurprisingly, the regulators' guidance generated results. Banks have withdrawn service from gun dealers that are existing customers, and denied others the ability to open accounts.[434] For example, a Wisconsin gun store owner recorded his conversation with a bank manager after the credit union closed his account.[435] Heritage Credit Union (HCU) employees told Mike Schuetz, the owner of Hawkins Guns, that "they do not service companies that deal in guns."[436] A regional manager for HCU elaborated that when examiners from the National Credit Union Administration audited the credit agency, they identified

-banks-business-with-payday-lenders.

430. *See* Editorial, *"Operation Choke Point" Hits the Mark*, N.Y. TIMES (Oct. 10, 2014), http://www.nytimes.com/2014/10/11/opinion/operation-choke-point-hits-the-mark.html.

431. FED. DEPOSIT INS. CORP., FINANCIAL INSTITUTION LETTERS, PAYMENT PROCESSOR RELATIONSHIPS REVISED GUIDANCE (Jan. 31, 2012), http://www.fdic.gov/news/news/financial/2012/fil12003.html.

432. *Id.*

433. *Managing Risks in Third Party Payment Processor Relationships*, FED. DEPOSIT INS. CORP. [hereinafter FED. DEPOSIT INS. CORP., *Managing Risks*] (June 21, 2011) (on file with the Minnesota Law Review).

434. *See* Mike Tobin, *DOJ Accused of Blocking Legal Gun Shops, Other Businesses from Banking*, FOX NEWS (Jan. 16, 2015), http://www.foxnews.com/politics/2015/01/16/doj-accused-blocking-legal-gun-shops-other-businesses-from-banking.

435. *See Hawkins Guns Targeted by Operation Choke Point*, U.S. CONSUMER COALITION, http://usconsumers.org/hawkinsguns (last visited Oct. 14, 2015) (providing recordings by Hawkins Guns owner).

436. Chuck Ross, *Audio Tapes Reveal How Federal Regulators Shut Down Gun Store Owner's Bank Accounts*, DAILY CALLER (Jan. 14, 2015, 2:51 PM), http://dailycaller.com/2015/01/14/audio-tapes-reveal-how-federal-regulators-shut-down-gun-store-owners-bank-accounts.

Hawkins Guns' account, among others, as "some accounts that we feel that we're going to regulate you on."[437] While the number of firearms dealers affected is not known, there are numerous reports of similar experiences: existing customers dropped because they operated "high-risk" or "prohibitive business type[s]."[438] Jawboning banks over guns worked.

The federal government's theory regarding its authority to designate certain sectors as highly risky for banks' reputations is convoluted at best. The FDIC has considerable regulatory authority over banks since the agency insures consumers' deposits. Among other powers, the FDIC is authorized to police unfair or deceptive trade practices under Section 5 of the Federal Trade Commission Act.[439] And, Section 8 of the Federal Deposit Insurance Act permits the FDIC to terminate an insured depository institution's status if the entity is in an unsafe or unsound condition to continue operations.[440] The FDIC frequently issues informal guidance to depository institutions, including regarding risk to their reputations that could damage their business.[441] In considering the risks that may be created via bank relationships with third parties, the FDIC includes reputation risk, which it defines as "the risk arising from negative public opinion."[442] Significantly, reputation risk can result from "[a]ny negative publicity involving the third party, whether or not the publicity is related to the institution's use of the third party."[443] Thus, as an outgrowth of its mandate to ensure

437. *Id.*

438. *See, e.g.*, Trevor Anderson, *Owner Believes His Pawn Shop Was Dropped by Bank for Selling Guns*, GOUPSTATE (Aug. 9, 2014, 10:14 PM), http://www.goupstate.com/article/20140809/articles/140809663; Kelly Riddell, *"High Risk" Label from Feds Puts Gun Sellers in Banks' Crosshairs, Hurts Business*, WASH. TIMES (May 18, 2014), http://www.washingtontimes.com/news/2014/may/18/targeted-gun-sellers-say-high-risk-label-from-feds (citing examples and stating that thousands of gun shop owners are affected).

439. 15 U.S.C. § 45(a) (2012); FED. DEPOSIT INS. CORP., GUIDANCE ON UNFAIR OR DECEPTIVE ACTS OR PRACTICES, FIL-57-2002 (May 30, 2002), https://www.fdic.gov/news/news/financial/2002/fil0257.html.

440. 12 U.S.C. § 1818(a)(2)(A)(ii)–(a)(3) (2012).

441. *See, e.g.*, FED. DEPOSIT INS. CORP., FEDERAL TRADE COMMISSION ACT, SECTION 5: UNFAIR OR DECEPTIVE ACTS OR PRACTICES, COMPLIANCE EXAMINATION MANUAL (2014), https://www.fdic.gov/regulations/compliance/manual/7/VII-1.1.pdf; FED. DEPOSIT INS. CORP., THIRD PARTY RISK, COMPLIANCE EXAMINATION MANUAL VII-4.2 (2014), https://www.fdic.gov/regulations/compliance/manual/7/VII-4.1.pdf (defining reputation risk).

442. FED. DEPOSIT INS. CORP., THIRD PARTY RISK, *supra* note 441.

443. *Id.*

that federally-insured depository institutions do not undertake excessive risk, the FDIC has both established categories of risk and then defined the substance of those categories.

Reputation risk is seemingly boundless: any entity that suffers bad publicity and that does business with a depository institution potentially creates legally actionable risk for that bank. Lawyers who advise banks have taken notice; one attorney described the term as "a catch-all to challenge any banking businesses that are disfavored."[444] At minimum, the FDIC failed to link the factors it identifies as indicating a high-risk client—the consumer's unfamiliarity with the merchant, uncertain quality of goods or services, purchases by phone or Internet, and inability of the consumer to verify the identity or legitimacy of the seller—to firearms and ammunition sales.[445] Thus, the FDIC's authority to designate arbitrarily particular lines of business as high-risk is questionable at best.

The Obama administration doubled down on jawboning banks with Operation Choke Point. Choke Point was designed to investigate banks and payment processors that might be knowingly transacting with businesses committing fraud.[446] Under the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA), the Attorney General can issue subpoenas to investigate fraudulent activity that affects a federally-insured financial institution.[447] With Choke Point, the administration used threats of subpoenas to pressure banks that do business with gun dealers. However, it is unclear whether activities by the bank itself can support an investigation under FIRREA. The Department of Justice's theory hangs upon a single district court case involving an alleged scheme by bank employees to misrepresent the prices of standing instruction trading to customers.[448] Related case law, such as that interpreting the relevant FIRREA language in other statutory

444. Peter Weinstock, *Examiners' Growing Misuse of "Reputation Risk*,*"* AM. BANKER (July 2, 2013), http://www.americanbanker.com/bankthink/examiners-growing-misuse-of-reputation-risk-1060329-1.html.

445. FED. DEPOSIT INS. CORP., *Managing Risks*, *supra* note 433.

446. *See* Alan Zibel, *DOJ: "Choke Point" Isn't Targeting Legal Gun Dealers, Payday Lenders*, WALL ST. J. MONEYBEAT (July 15, 2014, 2:47 PM), http://blogs.wsj.com/moneybeat/2014/07/15/doj-operation-choke-point-isnt-targeting-gun-dealers-payday-lenders.

447. 12 U.S.C. § 1833a(c)(2), 1833a(g) (2012).

448. *See* United States v. Bank of N.Y. Mellon, 941 F. Supp. 2d 438 (S.D.N.Y. 2013).

provisions, is split on the point.[449] A memo from the Director of the Consumer Protection Branch to Assistant Attorney General Stuart Delery noted the mixed precedent regarding the government's position, but stated that the Department of Justice would continue to rely on that single district court case to pursue its investigations.[450] Even if the Department's theory is correct, its approach under Operation Choke Point extended the logic by yet another step. The court case the Department cited involved allegedly fraudulent activities by employees of the depository institution.[451] With Choke Point, the Department of Justice threatened banks with liability merely for doing business with high-risk clients, apparently including gun firms—a far more tenuous connection to wrongdoing, if in fact there was any wrongdoing at all.[452]

Put simply, the combination of the FDIC's extension of its supervisory role into designating certain types of business as untouchable, and the extension of the Department of Justice's use of investigatory powers under FIRREA to attack not fraud, but relationships with the high-risk clients designated by the FDIC, put the government far afield from its statutory authority. Any one of these leaps might be permissible, but all of them risk asking us to believe six impossible things before breakfast, and may well constitute jawboning.[453]

The doctrinal parallels between First and Second Amendment constraints upon regulation, and the recent informal pressures on banks to achieve firearms policy goals, suggest

449. *See* United States v. Agne, 214 F.3d 47 (1st Cir. 2000).

450. Memorandum from Michael S. Blume, Dir., Consumer Prot. Branch, U.S. Dep't of Justice, to Stuart F. Delery, Assistant Attorney Gen., Civil Div., U.S. Dep't of Justice, Operation Choke Point: Six-Month Status Report 336–38 (Sept. 9, 2013), http://oversight.house.gov/wp-content/uploads/2014/05/Appendix-1-of-2.pdf.

451. *Bank of N.Y. Mellon*, 941 F. Supp. 2d at 443.

452. A staff report for the U.S. House of Representatives Committee on Oversight and Government Reform made similar allegations. U.S. HOUSE OF REPS., COMM. ON OVERSIGHT AND GOV'T REFORM, THE DEPARTMENT OF JUSTICE'S "OPERATION CHOKE POINT": ILLEGALLY CHOKING OFF LEGITIMATE BUSINESSES? (May 29, 2014), http://oversight.house.gov/wp-content/uploads/2014/05/Staff-Report-Operation-Choke-Point1.pdf; *see also* Emily Miller, *DOJ Accused of Targeting Gun Industry with "Choke Point" Program*, FOX NEWS (June 2, 2014), http://www.foxnews.com/politics/2014/06/02/holder-justice-department-accused-gun-grab-with-choke-point-program.

453. *Cf.* LEWIS CARROLL, THROUGH THE LOOKING GLASS, ch. V, (2013), http://www.gutenberg.org/files/12/12-h/12-h.htm (quoting the White Queen, who said, "sometimes I've believed as many as six impossible things before breakfast").

that this Article's theoretical approach to jawboning has application beyond the Internet context.

B. MAPPING NEW JAWBONING TERRITORY

A core scholarly question for jawboning, and other legislative threats, is whether, and, if so, when, these tactics are permissible once a government finds itself in uncharted territory. The example of jawboning about gun sales suggests a potential path through the contentious debates in the literature on regulatory threats—one that I will develop in future work, but outline here.[454] Put simply, the legitimacy of jawboning is likely to vary inversely with the level of structural constraint upon governmental regulation. Where barriers to regulation are relatively strong, as with enumerated rights including the First and Second Amendments, informal efforts are less likely to be legitimate.[455] Here, the Constitution deliberately hobbles government efforts. Even if jawboning evades judicial proscription, we should regard it as normatively problematic. Where there are intermediate barriers—such as regulations that draw intermediate scrutiny, including sex-based classifications,[456] or perhaps the unconstitutional conditions doctrine[457]—informal enforcement has some legitimate room to operate, though its use still ought to create a strong presumption against its permissibility.

In zones where governmental intervention requires only the most minimal substantiation under the rational basis test, perhaps jawboning ought to be presumptively permissible.[458] Here, informal enforcement can save costs to both regulator and regulated. The state could likely obtain authority with relative ease, and thus jawboning enables targets to comply more

454. This framework contrasts with how other scholars have approached these questions. Tim Wu, for example, views the legitimacy of regulatory threats as determined by whether an industry changes rapidly or slowly. Wu, *supra* note 49. Others view them as either in, or out. This Article's approach is more nuanced.

455. *See* District of Columbia v. Heller, 554 U.S. 570, 634–35 (2008).

456. *See* United States v. Virginia, 518 U.S. 515 (1996) (applying intermediate scrutiny to male-only admission policy at state military college).

457. *See* Renée Lettow Lerner, *Unconstitutional Conditions, Germaneness, and Institutional Review Boards*, 101 NW. U. L. REV. 775, 784–85 (2007) (drawing analogy between analysis in unconstitutional conditions cases and those involving sex-based distinctions).

458. *See generally* Williamson v. Lee Optical of Okla., Inc., 348 U.S. 483 (1955); Bambauer & Massaro, *supra* note 257.

easily, and government to effectuate its ends with fewer formalities. A key factor here is the capability and willingness of courts to patrol for defects in the political process, such as capture or public choice problems, that indicate a likely asymmetry between the government's ability to obtain results informally versus through rulemaking or legislative mechanisms.[459] This is no easy task, but it is one to which courts have historically been attuned in their role as countermajoritarian check on the other two branches.[460]

There are important tensions beneath the surface of this tentative schema. It is difficult to detect, for example, whether a regulation that affects speech draws (or ought to draw) First Amendment review.[461] Legal scholarship sharply contests the boundaries of speech protection, or eligibility, and while the Supreme Court has moved in the direction of greater coverage, it has not done so consistently.[462] In both the intermediate and light zones, deciding upon a methodology for how strong the presumption for or against jawboning ought to be is challenging. Courts have struggled with conceptually similar undertakings when defining tests for the unconstitutional conditions doctrine,[463] substantive due process violations,[464] or permissible gender-based discrimination.[465] And the approach may have significant consequences (albeit only suasive ones) for widespread practices such as plea bargains,[466] police interrogation,[467]

---

459. *See* United States v. Carolene Prods. Co., 304 U.S. 144, 152 n.4 (1938); Mark A. Graber, *The Countermajoritarian Difficulty: From Courts to Congress to Constitutional Order*, 4 ANN. REV. L. & SOC. SCI. 361, 363–65 (2008).

460. *See Carolene Prods. Co.*, 304 U.S. at 152 n.4; ALEXANDER M. BICKEL, THE LEAST DANGEROUS BRANCH 131–32 (1962). *But see* Jeremy Waldron, *The Core of the Case Against Judicial Review*, 115 YALE L.J. 1346 (2006) (criticizing judicial review as an illegitimate process for a democracy to protect rights).

461. *See generally* United States v. Caronia, 703 F.3d 149 (2d Cir. 2012); Collins, *supra* note 304.

462. *See generally* Bambauer, *supra* note 44; Collins, *supra* note 304; Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149 (2005).

463. *See supra* notes 363–64.

464. *See* Bambauer & Massaro, *supra* note 257.

465. *See* Norman T. Deutsch, Nguyen v. INS *and the Application of Intermediate Scrutiny to Gender Classifications: Theory, Practice, and Reality*, 30 PEPP. L. REV. 185, 191–212 (2003).

466. *See generally* Stephen J. Schulhofer, *Plea Bargaining as Disaster*, 101 YALE L.J. 1979 (1992).

467. *See generally* Deborah Young, *Unnecessary Evil: Police Lying in Interrogations*, 28 CONN. L. REV. 425 (1996).

and unfair competition enforcement.[468] It is also worth noting that this methodology comes into play when the state is acting at the edges of, or beyond, its authority to enforce or adjudicate. In the mine run of cases, such as Securities and Exchange Commission enforcement of securities laws,[469] or much of criminal law prosecution,[470] informal settlements will be both legitimate and desirable.

Nonetheless, this Part's proposed framework performs at least three valuable services. First, it offers a potential internal metric for regulators trying to determine when to pressure firms. When state actors are considering whether and how to press against the edges of their authority, this approach can guide them on when to employ formal rulemaking or adjudication, versus when to deploy informal measures. Second, it gives non-state entities—such as civil society groups, scholars, and regulatory targets themselves—a yardstick by which to evaluate state action.[471] It binds criticism to a methodology, which can answer objections that disapprobation is ad hoc or born of self-interest. Lastly, it draws attention to the distinction between law and mores. Not all permissible state actions are defensible.[472] This seems particularly true with regulation of information, whether by proscription, prescription, or persuasion. This Article usefully unsettles assumptions about the legitimacy of informal pressures.

Jawboning of Internet intermediaries is increasingly common, and it operates beneath the notice of both courts and commentators. That inattention is misguided. There are times when we need to root for Goliath.

---

468. *See generally* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014), *aff'd*, No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015); *see* Solove & Hartzog, *supra* note 337.

469. *See generally* Joshua A. Naftalis, Note, *"Wells Submissions" to the SEC as Offers of Settlement under Federal Rule of Evidence 408 and Their Protection from Third-Party Discovery*, 102 COLUM. L. REV. 1912 (2002).

470. *See* BUREAU OF JUSTICE ASSISTANCE, U.S. DEP'T OF JUSTICE, PLEA AND CHARGE BARGAINING: RESEARCH SUMMARY 1 (2011), https://www.bja.gov/Publications/PleaBargainingResearchSummary.pdf (estimating 90–95% of criminal cases settle).

471. *See* Bambauer, *Cybersieves*, *supra* note 258, at 386–87.

472. *See generally* Bambauer, *Orwell's Armchair*, *supra* note 58.