Maryland Law Review

Volume 79 | Issue 1 Article 6

Six Horsemen of Irresponsibility

Frank Pasquale

SIX HORSEMEN OF IRRESPONSIBILITY

FRANK PASQUALE*

There is now enormous controversy in the United States over internet intermediary responsibility for online content, ranging from guns to hate speech.[1] This controversy often focuses on Section 230 of the Communications Decency Act ("CDA 230"),[2] which Eric Goldman has called "[b]etter [t]han the First Amendment" to protect many online intermediaries from lawsuits, because "a defendant can win a motion to dismiss even when a plaintiff alleges that the defendant knew about—or intended—the allegedly illegal content."[3] In this brief piece, I do not intend to address the proper interpretation of CDA 230, or other laws. What I wish to do instead is to address synergistic effects rarely commented on in doctrinally siloed spaces of legal scholarship. Namely, what happens when laws like CDA 230 combine with or reinforce other immunizing doctrines, whether derived from federal or state constitutions, statutes, or common law? Is there any systematic way to reconsider the legal field as a whole, once such synergies against accountability are noticed?

In the course of teaching and writing about law and technology over the past decade, I have noticed no fewer than six "horsemen of irresponsibility" taking on important roles in technological contexts.[4] These include (1) contractual limitations on liability, including exculpatory and forced arbitration

* Piper & Marbury Professor of Law, University of Maryland. I wish to thank Mark Graber and participants at his annual constitutional law "schmooze" for permitting me to present this work. The workshop spurred valuable reflections on constitutional law and technology. I also wish to thank Sue McCarty and Jennifer Chapman for assistance in research and preparation of the piece.

1. Daniel v. Armslist, LLC, 926 N.W.2d 710, 714 (Wis. 2019) (holding intermediary not responsible for gun distribution facilitated by its site); Frank Pasquale, *The Automated Public Sphere*, *in* THE POLITICS OF BIG DATA: BIG DATA, BIG BROTHER? 110 (Ann Rudinow Sætnan et al. eds., 2018) (describing controversies over hate speech).

2. 47 U.S.C. § 230 (2012).

3. Eric Goldman, *Wisconsin Supreme Court Fixes a Bad Section 230 Opinion*—Daniel v. Armslist, TECH. & MARKETING L. BLOG (May 7, 2019), https://blog.ericgoldman.org/archives/2019/05/wisconsin-supreme-court-fixes-a-bad-section-230-opinion-daniel-v-armslist.htm.

4. This framing is inspired by SCOTT VEITCH, LAW AND IRRESPONSIBILITY: ON THE LEGITIMATION OF HUMAN SUFFERING (2007), and, more fancifully, by the classic cultural trope of "The Four Horsemen of the Apocalypse." *Revelation* 6:1–8. The term "apocalypse" in common parlance denotes end-times, but is also etymologically rooted in concepts of "revealing" or "unveil-

clauses; (2) expansive free expression claims; (3) trade secrecy; (4) intermediary immunities (such as CDA 230); (5) deregulation; and (6) preemption. These doctrines may each, individually or in narrow alliances, offer commendable liberties to technological innovators. However, they now have been collectively weaponized to eviscerate accountability for many firms' wrongdoing (or, worse, have made it impossible for outsiders to even discover the wrongdoing). Until a new balance has been struck, courts should be extremely wary of expanding any of these categories of immunity lest they unintentionally enhance their already extraordinary collective effect.

I. BARRIERS TO RESPONSIBILITY ONLINE

For an example of the troubling collective effect of these doctrines of legal irresponsibility, consider a public goal as simple and commendable as assuring that state actors or powerful oligarchs do not engage in massive manipulation of online platforms (like Facebook, Twitter, and Google) by deploying bots that emit propaganda or lies, spam hashtags with unrelated content, or post fake reviews or enable fake views on videos and other spaces for user-generated content. There are numerous ways to reduce the reach and influence of such bots. However, the six horsemen of irresponsibility, either individually or collectively, may render these efforts toothless.

For example, lawmakers may wish to force platforms to disclose exactly how they treat suspected bot accounts. However, the platforms can opportunistically deploy trade secrecy laws to argue that such disclosure is a taking of their intellectual property and data. Indeed, such expansive trade secrecy protections already hamstring much of freedom of information law, whether as statutory carve-outs, or as potential assertions of a constitutionally protected property right in court.

Another, more dramatic step would be to ban all bots on platforms. But such a move would almost certainly be met with a First Amendment challenge, thanks to precedents protecting certain forms of machine speech. A much less restrictive measure is to simply require accounts to disclose if they are run, in whole or in part, by a bot. California's recent legislative intervention to require bot disclosure is a case in point.[5] The law requires the owners and operators of bot accounts intended to affect elections or commercial

---

ing." My contention in this brief piece is that a critical mass of immunizing doctrines may effectively end the legal regimes of responsibility they ostensibly merely limit, revealing the fragility of legal protections of individuals, with apocalyptic consequences for those harmed.

5. Bolstering Online Transparency Act, CAL. BUS. & PROF. CODE §§ 17940–43 (West 2019). For a rationale for requiring disclosure in such cases, see Frank Pasquale, *Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society*, 78 OHIO ST. L.J. 1243, 1252–54 (identifying the "attribution problem" in robotics and artificial intelligence law and policy).

transactions, to disclose that the account is not operated directly by a human.[6] But even it might be challenged as "compelled" speech.

This California law reflects exactly the type of legal requirement necessary to assure minimally regulable technology in rapidly advancing technologies. Still, it is weaker than it needs to be, in part because of preemptive complaints about its potential effects on free expression (while the law was still a bill).

CDA 230 complicates other approaches to the problems posed by many troubling bots. Consider, for instance, the misinformation that could spread thanks to bots programmed to deliver anti-vaccine content, which could sow confusion about the benefits and risks of vaccinations on almost any post, video, or article about such issues. Despite repeated complaints about such content, a platform may look the other way, perhaps because it does not want to pay for workers to review such content, or because it wants to profit from it. Legislators might consider clearly imposing liability to make platforms responsible for harms caused by viral bot speech, especially after repeated complaints and warnings. But CDA 230 immunizes platforms from such liability for user generated content, and preempts well-intentioned state efforts to impose even minimal responsibility in these cases. And even if CDA 230 is partially or wholly repealed, it is possible that state contract law would recognize as binding terms of service that included exculpatory clauses for platforms. Given many large platforms' monopolistic power, such terms of service govern broad swathes of life online.

This panoply of self-reinforcing and layered doctrines of irresponsibility renders federal and state governments powerless to adequately defend the public sphere, just at the moment when technologies of deception, manipulation, and fraud are rapidly expanding in scope and intensifying in effect. Thanks to the advancing technology of "deepfakes," faces, voices, and other elements of human identity may be increasingly easily mimicked mechanically. Even "shallowfakes," such as obvious appropriations of others' images easily detected by a reverse image search, may spread misleading impressions. This potential for a public sphere increasingly unmoored from reality is particularly dangerous as bots become better at mimicking actual humans.

Despite being protected in the name of "free speech," many bots are intended to make collective will formation and authentic discussion impossible. Without a clear common sense of who is participating in the public sphere, and how, democratic dialogue declines in legitimacy. There is a growing body of empirical research on the troubling effects of an automated public sphere.[7] In too many scenarios, bot interventions are less speech than

6. *Id*.

7. *See, e.g.*, YOCHAI BENKLER ET AL., BERKMAN KLEIN CTR., PARTISANSHIP, PROPAGANDA, & DISINFORMATION: ONLINE MEDIA & THE 2016 U.S. PRESIDENTIAL ELECTION 17 (2017),

anti-speech, calculated efforts to disrupt democratic will formation or fool the unwary. Given growing concern about the extraordinary power of secret algorithmic manipulation to target influential messaging to persons with little to no appreciation of its ultimate source, courts should not privilege algorithmic data processing in these scenarios as speech worthy of the level of protection traditionally granted to political or even commercial speech.

To restore public confidence in democratic deliberation, authorities could require a license for using certain types of bots, akin to time, place, and manner restrictions on demonstrations. Despite protections of speech and assembly in the United States, protesters are not allowed to simply take over even public spaces at any time, with any level of noise, and with any number of persons. Rather, permits are often required. While such permitting may be manipulated in untoward ways, such a balance must be struck, lest the banner of "free speech" cloak and excuse all manner of lawlessness and nuisance. We might even think of a bot as a particularly noxious loudspeaker or long-range acoustic device, often restricted or banned to protect public order.

Authorities should also consider banning certain types of manipulation. The United Kingdom Code of Broadcast Advertising states that "audiovisual commercial communications shall not use subliminal techniques."[8] There is a long line of U.S. Federal Trade Commission ("FTC") guidance forbidding misleading advertisements and false or missing indication of sponsorship.[9]

---

https://dash.harvard.edu/bitstream/handle/1/33759251/2017-08_electionReport_0.pdf?sequence=9&isAllowed=y (examining "the dynamics of the [U.S. presidential] election by analyzing over two million stories related to the election, published online . . . [finding] the American political system has seen not a symmetrical polarization of the two sides of the political map, but rather the emergence of a discrete and relatively insular right-wing media ecosystem."); ROBYN CAPLAN ET AL., DATA & SOC'Y, DEAD RECKONING: NAVIGATING CONTENT MODERATION AFTER "FAKE NEWS" (2018), https://datasociety.net/pubs/oh/DataAndSociety_Dead_Reckoning_2018.pdf (discussing the negative impacts of "fake news" using data and research from the Media Manipulation Initiative at Data & Society Research Institute); ALICE MARWICK & REBECCA LEWIS, DATA & SOC'Y, MEDIA MANIPULATION AND DISINFORMATION ONLINE (2017), https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf (using research and data from the Data & Society Research Institute's Media Manipulation research group to examine how fringe, subculture messaging is amplified in the automated public sphere); LEE RAINIE ET AL., PEW RESEARCH CTR., THE FUTURE OF FREE SPEECH, TROLLS, ANONYMITY AND FAKE NEWS ONLINE 3 (2017), https://www.pewinternet.org/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online/ ("To illuminate current attitudes about the potential impacts of online social interaction over the next decade, Pew Research Center and Elon University's Imagining the Internet Center conducted a large-scale canvassing of technology experts, scholars, corporate practitioners and government leaders."); Frank Pasquale, *Reforming the Law of Reputation*, 47 LOY. U. CHI. L.J. 515 (2015) (describing effects of automated name search result queries on certain individuals).

8. THE BCAP CODE: THE UK CODE OF BROADCAST ADVERTISING 140 (2010), http://www.asa.org.uk/uploads/assets/uploaded/e6e8b10a-20e6-4674-a7aa6dc15aa4f814.pdf. The U.S. Federal Communications Commission has twice considered the issue, but done nothing.

9. *See, e.g.*, Guides Against Deceptive Pricing, 16 C.F.R. §§ 233.1–233.5 (2019); Guides Concerning Use of Endorsements and Testimonials in Advertising, 16 C.F.R. §§ 255.0–255.5 (2019).

Such federal law, as well as cognate state consumer protection law, should be supplemented to give private rights of action in the case of some particularly egregious bots whose misleading information causes concrete harms.[10] Given the FTC's manifold limitations, both the U.S. Congress, and states will need to develop more specific laws to govern an increasingly automated public sphere. For example, large platforms should be required to identify bot speech, to warn users about it, and to permit users to opt out of receiving it (or, better, should default all users to not be subject to bot speech, thus requiring users to affirmatively subject themselves to such communications).

II. THE SIX HORSEMEN AWAIT

There will be widespread resistance to such duties. Some proposals for preemption would severely diminish the role of state courts. Other enemies of intermediary responsibility would kneecap federal regulatory agencies, leaving it up to judges to determine *post hoc* the remedies appropriate for harm caused by AI. A final facet of "market ordering" would enable AI vendors to use exculpatory clauses in contracts to limit or shift their liability.[11]

Even more worryingly, certain constitutional protections for anonymous speech might effectively grant a "Ring of Gyges" to bot creators, rendering them invisible to potential plaintiffs or prosecutors no matter how much damage they cause. Some argue that bots deserve the right to generate expression online.[12] Free speech protection would likely include some right to anonymity, though that right has been limited in key contexts.[13] If a robust anonymity right compromises the ability of state actors to force disclosure of bot ownership, the First Amendment could effectively operate as a talismanic immunity for perpetrators of algorithmatized crime and torts. It could gut bot regulation.

Even if that particular Ring of Gyges fails to manifest, aggressive assertion of trade secrecy may provide another avenue for avoiding scrutiny. And

---

10. For examples of efforts to terrorize and harm individuals via online speech, which could be automated and put into bot form in an effort to evade responsibility, *see* CARRIE GOLDBERG, NOBODY'S VICTIM: FIGHTING PSYCHOS, STALKERS, PERVS, AND TROLLS (2019). Other examples could include bots promoting impure drugs, falsely reporting emergencies, or defaming individuals.

11. *See, e.g.*, Rebecca Crootof, *The Internet of Torts*, 69 DUKE L.J. (forthcoming 2019) (describing contractual clauses as a barrier to civil suits against technology companies).

12. *See, e.g.*, John Frank Weaver, *Why Robots Deserve Free Speech Rights*, SLATE (Jan. 16, 2018), https://slate.com/technology/2018/01/robots-deserve-a-first-amendment-right-to-free-speech.html ("By permitting the government to ban lawful speech, even A.I. speech, we eliminate a potentially useful voice. . . . The First Amendment protects the speaker, but more importantly it protects the rest of us, who are guaranteed the right to determine whether the speaker is right, wrong, or badly programmed. We are owed that right regardless of who is doing the speaking.").

13. *McConnell*, 540 U.S.at 93 (8-1 decision) (upholding disclosure requirements for campaign contributions); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995) (holding that the First Amendment protects a right to anonymous speech).

even if reformers overcome that hurdle to responsibility, expansive interpretations of CDA 230 of the Communications Decency Act might leave platforms utterly unaccountable for hosting anonymous accounts which blatantly violate laws requiring attribution, or stricter laws.

Each of these forms of legal irresponsibility is troubling on its own terms. Deregulatory legislation could compound their effects. For example, preempting state law to put bot regulation solely in the hands of the federal government would almost certainly be a mistake in the United States under the current administration, and would even be suspect under more enlightened rule.[14] To give just one example of the important information-forcing role of state law: tort litigation based on state-level common law can be critical to exposing information that may be blocked from regulators.[15] Barring some utterly discrediting governance failure, states should be entitled to develop their own standards for the level of risk they are willing to accept from emerging technologies (and emerging uses of older technologies).[16] Nor should they do so alone. Federal regulators play a vital role in gathering information to inform the public and state-level policymakers. Moreover, federal legislation can provide a baseline of protection for consumers, as the Health Insurance Portability and Accountability Act ("HIPAA") does with respect to health information.[17]

Some argue that "regulators could easily jump the gun in regulating AI, which would lead to irreparable harm in total welfare of human societies."[18] A supposed global AI arms race is a frequently given rationale here.[19] However, we are presumably competing to produce safe and accountable AI that

14. For a discussion of the Trump Administration's repeatedly arbitrary and capricious administrative action, see Fred Barbash & Deanna Paul, *The Real Reason the Trump Administration Is Constantly Losing in Court*, WASH. POST (Mar. 19, 2019, 12:05 PM), https://www.washingtonpost.com/world/national-security/the-real-reason-president-trump-is-constantly-losing-in-court/2019/03/19/f5ffb056-33a8-11e9-af5b-b51b7ff322e9_story.html?utm_term=.b08f95f19cbe.

15. Wendy Wagner, *When All Else Fails: Regulating Risky Products Through Tort Litigation*, 95 GEO. L.J. 695, 697–700, 711–13 (2007).

16. *See, e.g.*, JOHN VILLASENOR, PRODUCTS LIABILITY AND DRIVERLESS CARS: ISSUES AND GUIDING PRINCIPLES FOR LEGISLATION 16 (2014), https://www.brookings.edu/wp-content/uploads/2016/06/Products_Liability_and_Driverless_Cars.pdf ("To put it mildly, congressional preemption of state tort remedies with respect to autonomous vehicle liability would be a mistake. Liability for vehicle manufacturing defects has always been the province of state courts applying state tort remedies. That should continue to be the case for autonomous vehicles. While it is certainly true that state court remedies are sometimes inconsistent, it does not follow that the solution is for the federal government to strip state courts of their authority.").

17. *See* Frank Pasquale, *Grand Bargains for Big Data: The Emerging Law of Health Information*, 72 MD. L. REV. 653 (2013) (describing HIPAA's role in privacy protection). HIPAA acts as a baseline of privacy protection; states are free to add more protections.

18. Gonenc Gurkaynak et al., *Stifling Artificial Intelligence: Human Perils*, 32 COMPUTER L. & SECURITY REV. 749, 750 (2016).

19. Tristan Greene, *U.S. Government Is Clueless About AI and Shouldn't Be Allowed to Regulate It*, NEXT WEB (Oct. 24, 2017), https://thenextweb.com/artificial-intelligence/2017/10/24/us-

promotes a diverse and inclusive set of societal values. If we are not, we are in the wrong race.[20]

Another deregulatory strategy would be to "empower" the users of AI to contract away their rights to sue. The deontological case for contracts here is that they advance autonomy; the utilitarian case is that we may never have the data we need to make wise AI policy if vendors are afraid to try their wares outside the controlled environments of labs, without fear of liability. However, in certain contexts, a general suspicion of exculpatory clauses should prevail. For example, courts have frequently been unwilling to recognize such clauses in the medical context because patients are vulnerable, may lack the information necessary for a truly informed choice, and may be practically unable to switch providers at certain critical points of illness.[21] The field of AI development is highly technical, and poses many of the same types of information asymmetries and technical complexities that are common in medicine.[22] Even where such clauses are allowed, the courts still play an important role in policing unfair terms.[23] There are certain causes of action that should be preserved, whatever terms contracting parties are willing to agree to.[24]

Concededly, the policy debates in each of these areas are deep and complex. I can only scratch their surface in this short piece. But my intent is not to conclusively determine here whether any one of the six horsemen ((1) limitation of liability clauses; (2) expansive free expression claims; (3) trade secrecy; (4) intermediary immunities; (5) deregulation; and (6) preemption) is illegitimate in particular contexts. Rather, I am focusing on the heretofore little-remarked *synergy* of all these forms of legal irresponsibilization.[25] Any

government-is-clueless-about-ai-and-shouldnt-be-allowed-to-regulate-it/ ("Regulation could destroy America's chances in the AI race—a sprint it doesn't have a head start in, thanks to China's all-in policy. If the Trump administration sees fit to place restrictions on AI development that hamper Silicon Valley's ability to compete with Beijing, it'll lose more than just market shares. It could lose military superiority over countries like China and Russia.").

20. Virginia Dignum, *There Is No AI Race—and If There Is, It's the Wrong One to Run*, ALLAI, http://allai.nl/there-is-no-ai-race/ (last visited Aug. 6, 2019).

21. See, for example, *Tunkl v. Regents of the University of California*, 383 P.2d 441 (Cal. 1963), in which the court found a release signed by a patient as a condition of admission to a California research hospital invalid as against public policy due to unequal bargaining and lack of choice, and its progeny. *See also* Nadia N. Sawicki, *Choosing Medical Malpractice*, 93 WASH. L. REV. 891, 913 (2018) (finding that "courts are still quite resistant to any attempt by providers to minimize their liability on the basis of a patient's voluntary agreement, or to modify the default rules of the doctor-patient relationship by way of contractual agreement").

22. Frank Pasquale, *Data-Informed Duties for AI Development*, 119 COLUM. L. REV. (forthcoming 2019).

23. MARGARET JANE RADIN, BOILERPLATE 123–42, 138–40 (2013).

24. For an example of such insistence on the preservation of certain causes of action, see Douglas Andrew Grimm, *Informed Consent for All! No Exceptions*, 37 N.M. L. REV. 39 (2007). Such an approach might also disfavor blanket consents or compound authorizations.

25. I understand the aesthetic offense this nominalization may cause. However, it is intended as a counterpart to Professor Nikolas Rose's account of "responsibilization" in his theory of the

one of them could act to effectively eviscerate the force of laws with powerful public policy rationales. Together, they pose almost-insuperable barriers to accountability in critical technological contexts.

Lawyers and judges in the United States are often skilled at analysis (breaking a phenomenon or cause of action into constituent parts, or elements), but oft-adrift when it comes to synthesis (articulating a more comprehensive picture of reality, over extensive space or time). Specialization obscures the big picture. For example, in the case of internet companies, cyber lawyers too often confine themselves to recommending that major platforms like Google and Facebook should win key copyright cases, and trademark cases, and antitrust cases, and be granted certain First Amendment immunities, and not be classified as a "consumer reporting agency" under relevant privacy laws, and so on. They may well be correct in particular areas. But what happens when a critical mass of close cases combines with network effects to give a few firms unprecedented power over our information about (and even interpretation of) events?

Similar dynamics afflict finance. Old banking laws may fit poorly with aspects of the new, globalized financial (and fintech) landscape. There are numerous articles and position papers that attempt to dismantle the logic of Dodd-Frank, Basel, Sarbanes-Oxley, and other efforts to regulate high finance.[26] But if too-big-to-fail firms keep growing bigger, assured of state support, while regulation flounders, the social contract frays. As a Burkean, Oakeshottean, or Chestertonian conservatism would counsel: before upending a regulatory regime, lawmakers, regulators, and judges should carefully consider its purpose, function, and value. Even when empowered by one or more of the "six horsemen" above to limit firms' accountability, they should hesitate to do so.

human sciences. *See, e.g.*, Nikolas Rose, *Government and Control*, 40 BRIT. J. CRIMINOLOGY 321, 324, 328–29, 334 (2000). To build on an insight of Nicole Dewandre's: We may eventually tell a *longue durée* story of law in the long twentieth century as a progressive imposition of responsibilities on disempowered individuals, and grant of irresponsibility to hyper-empowered corporations (artificial persons) and robots (animated by artificial intelligences). Nicole Dewandre, *The Human Condition and the Black Box Society*, B2O (Dec. 16, 2015), https://www.boundary2.org/2015/12/dewandre-on-pascal/ (reviewing FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015)).

26. *See, e.g.*, David D. Schein & James D. Phillips, *Dodd-Frank: Consumers' Friend or Another D.C. Con Job?*, 2 BUS. & FIN. L. REV. 140, 160 (2019) ("[T]he dead weight of Dodd-Frank should be lifted and the agencies already charged with enforcement must be held to a much higher standard and actually follow their mandates.").

Lawyers of the Progressive Era and the New Deal dealt with challenges similar to those we face today: massive firms that warped the fabric of economic, political, and even cultural life to their own advantage.[27] They consulted the best of social science to recommend new, broader, and more comprehensive regulation. They may have sometimes gone too far, and each of the "six horsemen" mentioned above have played some role in limiting regulatory overreach. However, they now threaten to undo entire regulatory and liability regimes, and must be reined in.

The great promise of legal scholarship has been the thoughtful work of a body of professionals drawing from many disciplines to offer integrated, considered judgments about how to resolve disputes. Collectively, the six horsemen of legal irresponsibility short-circuit that process, particularly in the digital realm. We must be wary of efforts to further extend their power and scope.

27. Laura Kalman, *Law, Politics, and the New Deal(s)*, 108 YALE L.J. 2165, 2168–85 (1999); Paul Kens, *The Constitution and Business Regulation in the Progressive Era: Recent Developments and New Opportunities*, 56 AM. J. LEGAL HIST. 97, 97 (2016).