Written Testimony of

Frank Pasquale

Professor of Law

University of Maryland

Before the United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Digital Commerce and Consumer Protection

"Algorithms: How Companies' Decisions About Data and Content Impact Consumers"

November 29, 2017

"Algorithms: How Companies' Decisions About Data and Content Impact Consumers"

Written Testimony of Frank Pasquale[1]

I will answer the Committee's questions in order:

1) **How is personal information about consumers collected through the Internet, and how do companies use that information?**

Leading digital firms seek out intimate details of customers' (and potential customers') lives, but all too often try to give regulators, journalists, and the public at large as little information as they possibly can about their own statistics and procedures.[2] Internet companies collect more and more data on their users, but tend to fight many of the regulations that would let those same users exercise control over the resulting digital dossiers, and prevent discrimination based on them.

As technology advances, market pressures raise the stakes of the data game. Surveillance cameras become cheaper every year; sensors are embedded in more places.[3] Cell phones track our movements; programs log our keystrokes. Intensified data collection promises to make

[1] I wish to thank Sue McCarty and Jennifer Elisa Smith for help in compiling sources on very short notice, and to all those who responded to this request: https://twitter.com/FrankPasquale/status/935185521080455170. I was confirmed to testify on November 27 at about ten in the morning, and had to submit this written testimony by 10AM the next day. I therefore ask the reader's forgiveness for inconsistent footnote formatting and lack of comprehensive coverage of excellent work in algorithmic accountability now being done globally. I have based this testimony, in part, on previous work of mine covering the law and policy of big data, algorithmic accountability, and artificial intelligence.

[2] Frank Pasquale, *The Black Box Society* (Harvard University Press, 2015).

[3] Danielle Citron and Frank Pasquale, The Scored Society, *Wash. L. Rev.* (2014)

"quantified selves" of all of us, whether we like it or not.[4] The resulting information—a vast amount of data that until recently went unrecorded—is fed into databases and assembled into profiles of unprecedented depth and specificity.

But to what ends, and to whose? We are still only beginning to grapple with this problem. Empirical studies may document the value of narrow and particularized forms of profiling. But they only capture small facets of the tip of an iceberg of data use. What lies beneath is hidden via legal measures (such as trade secrecy), physical and administrative safeguards, and obfuscation. A growing algorithmic accountability movement is beginning to expose problems here, but it needs much more support from both government and civil society.[5]

The decline in personal privacy might be worthwhile if it were matched by comparable levels of transparency from corporations and government. But for the most part it is not. Credit raters, search engines, and major banks take in data about us and convert it into scores, rankings, risk calculations, and watch lists with vitally important consequences. But the proprietary algorithms by which they do so are all too often immune from scrutiny.[6]

The personal reputation business is exploding. Having eroded privacy for decades, shady, poorly regulated data miners, brokers and resellers have now taken creepy classification to a

[4] April Dembosky, "Invasion of the Body Hackers," *Financial Times,* June 10, 2011; Deborah Lupton, The Quantified Self (Polity, 2016); Jenifer S. Winter, "Surveillance in ubiquitous network societies: Normative conflicts related to the consumer in-store supermarket experience in the context of the Internet of Things." Ethics and Information Technology, 16(1), 27-41. doi:10.1007/s10676-013-9332-3.
[5] Frank Pasquale, *Digital Star Chamber*, at https://aeon.co/essays/judge-jury-and-executioner-the-unaccountable-algorithm (2015).
[6] Cathy O'Neil, Weapons of Math Destruction (2016); Frank Pasquale, Search, Speech, and Secrecy, at https://ylpr.yale.edu/inter_alia/search-speech-and-secrecy-corporate-strategies-inverting-net-neutrality-debates (2010).

whole new level.[7] They have created lists of victims of sexual assault, and lists of people with sexually transmitted diseases. Lists of people who have Alzheimer's, dementia and AIDS. Lists of the impotent and the depressed. There are lists of "impulse buyers." Lists of suckers: gullible consumers who have shown that they are susceptible to "vulnerability-based marketing." Even without such inflammatory data, firms can take advantage of unprecedented levels of other data about consumers. The result, as Ryan Calo demonstrates, is that "firms can not only take advantage of a general understanding of cognitive limitations, but can uncover, and even trigger, consumer frailty at an individual level."[8]

The growing danger of breaches challenges any simple attempts to justify data collection in the service of "consumer targeting." Even huge and sophisticated companies can be hacked, and cybercriminals' data trafficking is, unsurprisingly, an obscure topic.[9] In at least one case, an established U.S. data broker accidentally sold "Social Security and driver's license numbers—as well as bank account and credit card data on millions of Americans" to ID thieves.[10] Until data companies are willing to document and report the precise origins and destinations of all the data they hold, we will never be able to estimate the magnitude of data misuse. Moreover, as the

---

[7] Wolfie Christl, *How Companies Use Personal Data Against People: Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information* (2017); Theodore Rostow, What Happens When an Acquaintance Buys Your Data?, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2870044 (2016).

[8] Ryan Calo, Digital Market Manipulation, at http://www.gwlr.org/wp-content/uploads/2014/10/Calo_82_41.pdf; see also Ariel Ezrachi and Maurice Stucke, Is Your Digital Assistant Devious?, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2828117.

[9] Misha Glenny, *DarkMarket: How Hackers Became the New Mafia* (New York: Vintage Books, 2012) 2 ("this minuscule elite (call them geeks, technos, hackers, coders, securocrats, or what you will) has a profound understanding of a technology that every day directs our lives more intensively and extensively, while most of the rest of us understand absolutely zip about it.").

[10] "Experian Sold Consumer Data to ID Theft Service," *Krebs on Security*, October 20, 2013, http://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service/.

recent Equifax hack showed, massive reservoirs of personal data remain all too vulnerable to misuse.

Even when data is not breached, it can still disadvantage consumers. Think, for example, of the people who type words like "sick," "stressed," or "crying" into a search engine or an online support forum and find themselves in the crosshairs of clever marketers looking to capitalize on depression and insecurity.[11] Marketers plot to tout beauty protects at moments of the day that women feel least attractive.[12] There's little to stop them from compiling digital dossiers of the vulnerabilities of each of us.[13] In the hall of mirrors of online marketing, discrimination can easily masquerade as innovation.[14]

These methods may seem crude or reductive, but they are beloved by digital marketers. They are fast and cheap and there is little to lose. Once the data is in hand, the permutations are endless, and somebody is going to want them. If you're a childless man who shops for clothing online, spends a lot on cable TV, and drives a minivan, data brokers may well assume that you

[11] Ryan Calo, "Digital Market Manipulation," at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703&download=yes.

[12] PRNewsWire, "New Beauty Study Reveals Days, Times and Occasions When U.S. Women Feel Least Attractive," October 2, 2013 (news release), http://www.prnewswire.com/news-releases/new-beauty-study-reveals-days-times-and-occasions-when-us-women-feel-least-attractive-226131921.html.

[13] Paul Ohm coined the term "database of ruin" to suggest how damaging information could accumulate about a person. Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *University of California at Los Angeles Law Review* 57 (2010): 1750-51.

[14] Preston Gralla, Opinion, Amazon Prime and the Racist Algorithms, COMPUTERWORLD (May 11, 2016, 5:17 AM), https://www.computerworld.com/article/3068622/internet/amazon-prime-and-the-racist-algorithms.html ("In Amazon's mind, race has nothing to do with black neighborhoods being excluded, because no racial demographic data was used in its decision-making. But dig a little deeper, and you'll see that race has everything to do with it. . . . 'The Amazon algorithm operates off of an inherited cartography of previous redlining efforts, which created pockets of discrimination, the consequence being that the discrimination continues to be reproduced.'" (quoting Jovan Scott Lewis)).

are heavier than average.[15] And we now know that recruiters for obesity drug trials will happily pay for that analysis, thanks to innovative reporting.[16] But in most cases, we don't know what the owners of massive stores of data are saying about us.

Where does all this data come from? Everywhere. Have you ever searched for "flu symptoms" or "condoms"? That clickstream may be around somewhere, potentially tied to your name (if you were signed in) or the IP address of your computer or perhaps some unique identifier of its hardware.[17] It's a cinch for companies to compile lists of chronic dieters, or people with hay fever. "Based on your credit-card history, and whether you drive an American automobile and several other lifestyle factors, we can get a very, very close bead on whether or not you have the disease state we're looking at," said a vice president at a company in the health sector.[18] Consumers also worry about the potential misuse of "smart meter" and other technology.[19]

---

[15] Joseph Walker, "Data Mining to Recruit Sick People," *Wall Street Journal*, December 17, 2013, http://online.wsj.com/news/articles/SB10001424052702303722104579240140554518458. The *Journal* tries to explain these Big Data associations by hypothesizing that large men need minivans because they cannot fit into other vehicles. But note how easily we could also rationalize the opposite conclusion: if minivan drivers were pegged as exceptionally fit, we might hypothesize that they used the large vehicle to carry around sports equipment. We should beware post hoc rationalizations of Big Data correlations, particularly when we are unable to review the representativeness of the data processed or the algorithms used to process it.

[16] Ibid.

[17] Mary Ebeling, *Health Care and Big Data* (Polity, 2016). Some privacy protective measures are taken with respect to search logs. But, as Nissenbaum and Toubiana observe, "Without an external audit of these search logs, it is currently impossible to evaluate their robustness against de-anonymizing attacks." V. Toubiana and H. Nissenbaum, "An Analysis of Google Log Retention Policies," *The Journal of Privacy and Confidentiality* 3, no. 1 (2011): 5. For a search query revelation that proved revealing, despite anonymization efforts, see Thomas Barbaro and Michael Zeller, "A Face Is Exposed for AOL Searcher No. 4417749," *New York Times*, August 9, 2006, A1.

[18] Walker, "Data Mining to Recruit Sick People."

[19] Jenifer S. Winter, "(Un)ethical use of smart meters?" In S. Gangadharan (Ed.) Data and discrimination: Collected essays. (2014).

Some companies have assembled and sold the mailing addresses and medication lists of depressed people and cancer patients. A firm reportedly combined credit scores and a person's specific ailments into one report.[20] The Federal Trade Commission has been trying to nail down a solid picture of these practices,[21] but exchange of health data is an elusive target when millions of digital files can be encrypted and transmitted at the touch of a button.[22] We may eventually find records of data *sales,* but what if it is traded in handshake deals among brokers? A stray flash drive could hold millions of records. It's hard enough for the FTC to monitor America's brick-and-mortar businesses; the proliferation of data firms has completely overtaxed it.[23]

Unexpected and troubling uses of data abound. We already know that at least one credit card company has paid attention to certain mental health events, like going to marriage counseling.[24] When statistics imply that couples in counseling are more likely to divorce than couples who aren't, counseling becomes a "signal" that marital discord may be about to spill over into financial distress.[25] This is effectively a "marriage counseling penalty," and poses a dilemma for policy makers. Left unrevealed, it leaves cardholders in the dark about an important

---

[20] Julie Brill, "Reclaim Your Name," Keynote Address at Computers, Freedom, and Privacy Conference, June 26, 2013. Available at http://www.ftc.gov/speeches/brill/130626computersfreedom.pdf.

[21] FTC, "Data Brokers: A Call for Transparency and Accountability." Federal Trade Commission, May 2014.

[22] Ibid. ("One health insurance company recently bought data on more than three million people's consumer purchases in order to flag health-related actions, like purchasing plus-sized clothing, the *Wall Street Journal* reported. [The company bought purchasing information for current plan members, not as part of screening people for potential coverage.]")

[23] Peter Maass, "Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless," *Wired,* June 28, 2012, http://www.wired.com/threatlevel/2012/06/ftc-fail/all/.

[24] Charles Duhigg, "What Does Your Credit Card Company Know about You?" *New York Times,* May 17, 2009, http://www.nytimes.com/2009/05/17/magazine/17credit-t.html?pagewanted=all. For a compelling account for the crucial role that the FTC plays in regulating unfair consumer practices and establishing a common law of privacy, see Daniel J. Solove and Woodrow Hartzog, "The FTC and the New Common Law of Privacy," *Columbia Law Review* 114 (2014): 583–676.

[25] Duhigg, "What Does Your Credit Card Company Know about You?", New York Times.

aspect of creditworthiness. Once disclosed, it could discourage a couple from seeking the counseling they need to save their relationship.

There doesn't have to be any established causal relationship between counseling and late payments; correlation is enough to drive action. That can be creepy in the case of objectively verifiable conditions. And it can be devastating for those categorized as "lazy," "unreliable," "struggling," or worse. Runaway data can lead to *cascading disadvantages* as digital alchemy creates new analog realities. Once one piece of software has inferred that a person is a bad credit risk, a shirking worker, or a marginal consumer, that attribute may appear with decision-making clout in other systems all over the economy. There is little in current law to prevent companies from selling their profiles of you.[26]

Bad inferences are a larger problem than bad data because companies can represent them as "opinion" rather than fact. A lie can be litigated, but an opinion is much harder to prove false; therefore, it is much harder to dispute.[27] For example, a firm may identify a data subject not as an "allergy sufferer," but as a person with an "online search propensity" for a certain "ailment or prescription."[28] Similar classifications exist for "diabetic-concerned households." It may be easy for me to prove that I don't suffer from diabetes, but how do I prove that I'm not "diabetic-

[26] Kashmir Hill, "Could Target Sell Its 'Pregnancy Prediction Score'?" *Forbes*, February 16, 2012, http://www.forbes.com/sites/kashmirhill/2012/02/16/could-target-sell-its-pregnancy-prediction-score/.
[27] Frank Pasquale, "Reputation Regulation: Disclosure and the Challenge of Clandestinely Commensurating Computing," in *The Offensive Internet: Speech, Privacy, and Reputation*, ed. Saul Levmore and Martha C. Nussbaum (Cambridge, MA: Harvard University Press, 2010), 107–123; Frank Pasquale, "Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries," *Northwestern University Law Review* 104 (2010): 105–174.
[28] Lois Beckett, "Everything We Know about What Data Brokers Know about You," *ProPublica*, March 7, 2013 (updated September 13, 2013), http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you.

concerned"? And if data buyers are going to lump me in with diabetics anyway, what good does it do me even to bother challenging the record?

Profiling may begin with the original collectors of the information, but it can be elaborated by numerous data brokers, including credit bureaus, analytics firms, catalog co-ops, direct marketers, list brokers, affiliates, and others.[29] Brokers combine, swap, and recombine the data they acquire into new profiles, which they can then sell back to the original collectors or to other firms. It's a complicated picture, and even experts have a tough time keeping on top of exactly how data flows in the new economy.

Most of us have enough trouble keeping tabs on our credit history at the three major credit bureaus. But the Internet has supercharged the world of data exchange and profiling, and Experian, TransUnion, and Equifax are no longer the sole, or even the main, keepers of our online reputations. What will happen when we've got dozens, or hundreds, of entities to keep our eyes on?

We're finding out. They're already here, maintaining databases that, though mostly unknown to us, record nearly every aspect of our lives. They score us to decide whether we're targets or "waste," as media scholar Joseph Turow puts it.[30] They keep track of our occupations and preoccupations, our salaries, our home value, even our past purchases of luxury goods.[31]

---

[29] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012). Available at http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (providing list of types of data brokers).

[30] Joseph Turow, *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth* (New Haven, CT: Yale University Press, 2012).

[31] Natasha Singer, "Secret E-Scores Chart Consumers' Buying Power," *New York Times*, August 18, 2012.

(Who knew that one splurge on a pair of really nice headphones could lead to higher prices on sneakers in a later online search?) There are now hundreds of credit scores for sale, and thousands of "consumer scores," on subjects ranging from frailty to reliability to likelihood to commit fraud. And there are far more sources of data for all these scores than there are scores themselves.[32] Any one of them could change our lives on the basis of a falsehood or a mistake that we don't even know about.[33]

We also need to worry about how public and private databases bleed into one another, potentially reinforcing cycles of disadvantage.[34] Such sources can be based on biased data—for example, if police focus their efforts on minority communities, more minorities may end up with criminal records, regardless of whether minorities generally commit more crimes.[35] Researchers are revealing that online sources may be just as problematic. As the White House Report on Big Data has found, "big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace."[36] Already disadvantaged groups may be particularly hard hit.[37]

---

[32] Dixon and Gellman, *The Scoring of America.*

[33] Ylan Q. Mui, "Little-Known Firms Tracking Data Used in Credit Scores," *Washington Post,* July 16, 2011, http://www.washingtonpost.com/business/economy/little-known-firms-tracking-data-used-in-credit-scores/2011/05/24/gIQAXHcWII_print.html. The firm was ChoicePoint (now a part of another, larger firm), a data broker that maintained files on nearly all Americans.

[34] Danielle Keats Citron and Frank Pasquale, "Network Accountability for the Domestic Intelligence Apparatus," *Hastings Law Journal* 62 (2011): 1441–1494; Chris Jay Hoofnagle, "Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement," University of North Carolina Journal of International Law and Commercial Regulation 29 (2004): 595–638; Jon D. Michaels, "All the President's Spies: Private–Public Intelligence Partnerships in the War on Terror" (2008).

[35] Associated Press, "EEOC Sues over Criminal Background Checks," *CBSNews,* June 11, 2013, http://www.cbsnews.com/8301-505123_162-57588814/eeoc-sues-over-criminal-background-checks/.

[36] Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* (2014).

For example, consider one computer scientist's scrutiny of digital name searches. In 2012, Latanya Sweeney, former director of the Data Privacy Lab at Harvard and now a senior technologist at the Federal Trade Commission, suspected that African Americans were being unfairly targeted by an online service. When Sweeney searched her own name on Google, she saw an ad saying, "Latanya Sweeney: Arrested?" In contrast, a search for "Tanya Smith" produced an ad saying, "Located: Tanya Smith."[38] The discrepancy provoked Sweeney to conduct a study of how names affected the ads served. She suspected that "ads suggesting arrest tend to appear with names associated with blacks, and neutral ads or no [such] ads tend to appear with names associated with whites, regardless of whether the company [purchasing the ad] has an arrest record associated with the name." She concluded that "Google searches for typically African-American names lead to negative ads posted by [the background check site] InstantCheckmate.com, while typically Caucasian names draw neutral ads."[39]

After Sweeney released her findings, several explanations for her results were proposed. Perhaps someone had deliberately programmed "arrest" results to appear with names associated with blacks? That would be intentional discrimination, and Instant Checkmate and Google both vehemently denied it. On the other hand, let us suppose that (for whatever reasons) web

---

[37] David Talbot, "Data Discrimination Means the Poor May Experience a Different Internet," *Technology Review*, Oct. 9, 2013, at http://www.technologyreview.com/news/520131/data-discrimination-means-the-poor-may-experience-a-different-internet/ (discussing work of Kate Crawford and Jason Schultz).

[38] Devony B. Schmidt, "Researchers Present Findings on Online Criminal Record Websites," *The Harvard Crimson,* November 20, 2012, http://www.thecrimson.com/article/2012/11/20/research-finds-profiling/.

[39] Latanya Sweeney, "Discrimination in Online Ad Delivery," *Communications of the ACM* 56 (2013): 44. She ultimately found "statistically significant discrimination in ad delivery based on searches of 2184 racially associated personal names," in that ads suggesting arrest (as in the question, Arrested?) were likely to appear in the context of names associated with blacks even when there was no actual arrest record associated with the name. This was not true of names associated with whites. There are many more examples of very troubling, racially charged sorting in Safiya U. Noble, *Algorithms of Oppression* (forthcoming, 2018).

searchers tended to click on Instant Checkmate ads more often when names associated with blacks had "arrest" associations, rather than more neutral ones. In that case, the programmer behind the ad-matching engine could say that all it is doing is optimizing for clicks—it is agnostic about people's reasons for clicking.[40] It presents itself as a cultural voting machine, merely registering, rather than creating, perceptions.[41]

Given algorithmic secrecy, it's very hard to know exactly what's going on here.[42] Perhaps a company had racially inflected ad targeting; perhaps Sweeney's results arose from other associations in the data.[43] But without access to the underlying coding and data, it is very difficult to adjudicate the dispute. That is troubling, because as FTC chair Edith Ramirez has argued, we must "ensure that by using big data algorithms they are not accidentally classifying

[40] "Racism Is Poisoning Online Ad Delivery, Professor Says," *MIT Technology Review*, February 4, 2013, http://www.technologyreview.com/view/510646/racism-is-poisoning-online-ad-delivery-says-harvard-professor/.

[41] Toon Calders & Indre Zliobaite, "Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures," in *Discrimination and Privacy in the Information Society* (Bart Custers, et al., eds.) (Heidelberg: Springer, 2013).

[42] Trade secrecy will likely continue to blunt efforts to get to the bottom of issues like the ones identified by Sweeney. However, there are forms of auditing that can help us understand what is going on in automated systems without full transparency of data or algorithms. See, e.g. Christian Sandvig et al., Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms, at http://www-personal.umich.edu/~csandvig/research/Auditing%20Algorithms%20--%20Sandvig%20--%20ICA%202014%20Data%20and%20Discrimination%20Preconference.pdf; Sandra Wachter, Brent Mittelstadt, and Chris Russell, Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289.

[43] On the question of attribution and intent, see Frank Pasquale, Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3002546; Luciano Floridi, Faultless responsibility: on the nature and allocation of moral responsibility for distributed moral actions, at https://www.ncbi.nlm.nih.gov/pubmed/28336791.

people based on categories that society has decided—by law or ethics—not to use, such as race, ethnic background, gender, and sexual orientation."[44]

2) How do companies make decisions about content that consumers see online?

The same problems of opacity that plague the dark market in personal data, also afflict online content display and ordering. A large platform may marginalize (or entirely block) potential connections between audiences and speakers. Consumer protection concerns arise, for platforms may be marketing themselves as open, comprehensive, and unbiased, when they are in fact closed, partial, and self-serving. Responding to protests, accused platforms have tended both to assert a right to craft the information environments they desire, and to abjure responsibility, claiming to merely reflect the desires and preferences of the user base. Such contradictory responses betray an opportunistic commercialism at odds with the platforms' touted social missions. Large platforms should be developing (and holding themselves to) more ambitious standards, rather than warring against privacy, competition, and consumer protection laws.[45] These regulations enable a more vibrant public sphere. They also defuse the twin specters of monopolization and total surveillance, which are grave threats to freedom of expression.

Policymakers should also consider expanding some core principles of network neutrality beyond the physical layer of the internet to very large enterprises at the social, search, and app level.[46] Bottlenecks can threaten competition at any layer of the network.

[44] Ibid.
[45] Frank Pasquale, Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2779270 (2016).
[46] Frank Pasquale, Internet Nondiscrimination Principles: Commercial Ethics for Carriers and Search Engines, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1134159 (2008).

Renewed enforcement of anti-discrimination law is also critical in online contexts. One thing is clear: self-regulation is not working. As reported in ProPublica, after Facebook was caught enabling discriminatory housing ads online in 2016, it pledged to change its system to fix the problem. But the issue persists.[47]

The interaction between paid and organic search results also merits attention here.[48] Google's misadventures in the medical space suggest some of the problems that can arise when automated systems are not up to the tasks that they have taken on. According to a recent report, its neglect enabled predatory addiction clinics to displace more established ones, and may be making discrimination as to source of insurance coverage all too easy.[49] As a de facto addiction center referral center, it has effectively let bad actors game its systems. The company may plead that it is not responsible. But one has to wonder about whether its extraordinarily high profit levels are premised on a level of neglect of the vulnerable that is unacceptable.[50] An insurer that

[47] Julia Angwin, Ariana Tobin and Madeleine Varner, Facebook (Still) Letting Housing Advertisers Exclude Users by Race, at https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin. Angwin's series of articles on algorithmic bias at ProPublica, as well as her earlier "What They Know" series in the Wall Street Journal, are a vital resource for those interested in online discrimination. *What They Know*, at http://www.wsj.com/public/page/what-they-know-digital-privacy.html.

[48] For an account of extant regulation, see Frank Pasquale, Beyond Innovation and Competition, Northwestern L. Rev. (2010) (discussing the FTC's sponsorship disclosure guidelines); Danny Sullivan, A Letter To The FTC Regarding Search Engine Disclosure Compliance, at https://searchengineland.com/a-letter-to-the-ftc-regarding-search-engine-disclosure-124169 (discussing the need to ensure that FTC guidelines on sponsorship disclosure are actually enforced).

[49] Cat Ferguson, How Disreputable Rehabs Game Google to Profit off Patients, The Verge, at https://www.theverge.com/2017/9/7/16257412/rehabs-near-me-google-search-scam-florida-treatment-centers; David Dayen, Google is So Big, It is Now Shaping Policy to Combat the Opioid Epidemic—And Screwing it Up, The Intercept, at https://theintercept.com/2017/10/17/google-search-drug-use-opioid-epidemic/.

[50] Will Oremus, *Facebook's Broken Promises*, SLATE (Nov. 24, 2017, 9:47 AM), http://www.slate.com/articles/technology/technology/2017/11/why_facebook_broke_its_promise_to_stop_allowing_racist_housing_ads.html ("fixing these problems requires time, resources, and, yes, manpower—all of which not only cut into Facebook's profits but run counter to its entire culture and

maintained networks of manifestly incompetent or unqualified professionals could be either secondarily or directly liable for its failures. An online intermediary irresponsibility lobby has worked hard to entrench ever more expansive readings of Section 230 of the Communications Decency Act in order to immunize firms like Google from such responsibility. At some point, though, the collateral consequences of such policies need to be taken into account.[51]

The same concerns also arise in education and finance. As Sam Adler-Bell explains, "Debt relief companies are counting on you doing what most people do when a serious and complicated problem strikes: Google it. . . . [T]he CFPB [has] sent letters to Microsoft, Google, Facebook, and Yahoo warning them that student debt scammers were using their ad services and search products to 'lure distressed borrowers.'"[52] The college classroom itself may be stratified by big data in ways that are hard for students to fully understand.[53] Librarians and information science professionals are exposing the stakes of different algorithmic systems of ordering

---

philosophy."). On intermediary irresponsibility generally, see Frank Pasquale, The Automated Public Sphere, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3067552 (2017).

[51] There are some exceptions to talismanic 230 immunities. See, e.g., Jake Pearson, How a Career Con Man Led a Federal Sting that cost Google $500 million, at https://www.wired.com/2013/05/google-pharma-whitaker-sting/ ("As part of the agreement, the company acknowledged that it had helped presumably Canadian online pharmacies use AdWords as early as 2003, that it knew US customers were buying drugs through these ads, that advertisers were selling drugs without requiring prescriptions, and that Google employees actively helped advertisers circumvent their own pharmaceutical policies and third-party verification services.").

[52] Sam Adler-Bell, *Scam Artists are preying on Student Debt Holdres – and Google is Helping*, COMMENTARY: THE CENTURY FOUNDATION (Sept. 14, 2015), https://tcf.org/content/commentary/scam-artists-are-preying-on-student-debt-holders-and-google-is-helping/.

[53] Frank Pasquale, Big Data: It's Worse than you Thought, at http://www.latimes.com/opinion/op-ed/la-oe-0116-pasquale-reputation-repair-digital-history-20150116-story.html ("colleges are now using data to warn professors about at-risk students. Some students arrive in the classroom with a "red light" designation — which they don't know about, and which is based on calculations they can't access").

information.[54] And even at the earliest stages of education, algorithmic mediation is having widespread (and largely unexamined) effects.[55]

Ariel Ezrachi and Maurice Stucke have described the resulting online landscape as a version of the movie *The Truman Show*, where we are constantly manipulated in ways we can neither fully anticipate nor guard against.[56] Many users have little appreciation of the way that algorithms are shaping their online experience.[57] For example, Navneet Alang has reported that Amazon "uses AI to push customers to higher-priced products that come from preferred partners."[58] These methods may be becoming more widespread.[59] In their account of the "algorithmic consumer," Michael S. Gal & Niva Elkin-Koren conclude that:

---

[54] See, e.g., Algorithmic Bias in Library Discovery Systems, at https://matthew.reidsrow.com/articles/173; Moritz Hardt, How big data is unfair: Understanding unintended sources of unfairness in data driven decision making, at https://medium.com/@mrtz/how-big-data-is-unfair-9aa544d739de.

[55] Elana Zeide, The Structural Consequences of Big Data-Driven Education (June 23, 2017). Big Data, Vol 5, No. 2 (2017): 164-172, at https://ssrn.com/abstract=2991794 ("[B]ig data-driven tools define what 'counts' as education by mapping the concepts, creating the content, determining the metrics, and setting desired learning outcomes of instruction. These shifts cede important decision-making to private entities without public scrutiny or pedagogical examination. In contrast to the public and heated debates that accompany textbook choices, schools often adopt education technologies ad hoc.").

[56] Ben Schiller, You Are Being Exploited By The Opaque, Algorithm-Driven Economy, at https://www.fastcompany.com/40447841/you-are-being-exploited-by-the-opaque-algorithm-driven-economy.

[57] Motahhare Eslami et al., "I Always Assumed That I Wasn't Really That Close to [Her]": Reasoning About Invisible Algorithms in the News Feed, 2015 PROC. 33RD ANN. ACM CONF. ON HUM. FACTORS COMPUTING SYS. 153, available at: http://www-personal.umich.edu/~csandvig/research/Eslami_Algorithms_CHI15.pdf (Study focused on user engagement with Facebook's News Feed algorithm, finding "that 62.5% of participants were not aware of the algorithm's existence.").

[58] Navneet Alang, *Turns Out Algorithms are Racist*, NEW REPUBLIC (Aug. 31, 2017), https://newrepublic.com/article/144644/turns-algorithms-racist, citing Julia Angwin & Surya Mattu, Amazon Says It Puts Customers First. But Its Pricing Algorithm Doesn't, PROPUBLICA (Sept. 20, 2016, 8:00 AM), https://www.propublica.org/article/amazon-says-it-puts-customers-first-but-its-pricing-algorithm-doesnt).

[59] Katie Pedersen, Greg Sadler and Virginia Smart, *How Companies Use Personal Data to Charge Different People Different Prices for the Same Product*, CBC NEWS (Nov. 24, 2017, 2:21 PM),

> [V]ulnerability to biases and errors embedded in the code or drawn from the data is not easily overcome. A consumer who is unaware of such assumptions will likely also be unaware of any choices she has forgone. This type of failure, involving unknown unknowns, is likely to be difficult to fix. Consumers may find it increasingly difficult — or not worth their time — to exercise oversight over sophisticated and opaque systems.[60]

Rural or socioeconomically disadvantaged areas may be hardest hit.[61] Moreover, many consumers may not even believe they have to guard against price discrimination, because they assume it is illegal.[62] Or they may find it futile to even try to protect themselves against that and other forms of discrimination, given the opacity of contemporary data practices.[63] Fortunately,

---

http://www.cbc.ca/news/business/marketplace-online-prices-profiles-1.4414240; *Price-bots Can Collude Against Consumers*, THE ECONOMIST: FREE EXCHANGE BLOG (May 6, 2017), https://www.economist.com/news/finance-and-economics/21721648-trustbusters-might-have-fight-algorithms-algorithms-price-bots-can-collude.

[60] Michael S. Gal & Niva Elkin-Koren, *Algorithmic Consumers*, 30 HARV. J.L. & TECH. 309 (2017), available at: http://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech309.pdf.

[61] Jennifer Valentino-DeVries, Jeremy Singer-Vine & Ashkan Soltani, Websites Vary Prices, Deals Based on Users' Information, WALL ST. J. (Dec. 24, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534 ("using geography as a pricing tool can also reinforce patterns that e-commerce had promised to erase: prices that are higher in areas with less competition, including rural or poor areas. It diminishes the Internet's role as an equalizer.); Kaveh Waddell, The Internet May Be as Segregated as a City, THE ATLANTIC (Sept. 6, 2016), https://www.theatlantic.com/technology/archive/2016/09/the-internet-may-be-as-segregated-as-a-city/498608/.

[62] Neil Howe, A Special Price Just for You, FORBES (Nov. 17, 2017, 5:56 PM), https://www.forbes.com/sites/neilhowe/2017/11/17/a-special-price-just-for-you/#dfd7bce90b32 ("When consumers realize that price discrimination is occurring, they object. Most, in fact, mistakenly believe it to be illegal. A 2005 Annenberg Center study found that 64% of adult Internet users thought it was illegal for e-commerce sites to charge different prices to different customers—and 71% thought it was illegal for brick-and-mortar retailers to do so.").

[63] Mary Madden, Michele Gilman, Karen Levy & Alice Marwick, Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans, 95 WASH. U.L.R. 53 (2017), at https://openscholarship.wustl.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=6265&context=law_lawreview ("In cases of big-data-related decision-making and discrimination,

researchers are now documenting algorithmic biases to raise public awareness of them.[64] But this is a problem that individuals, on their own, cannot hope to solve. It has to be addressed by policymakers.

There is a range of responses that policymakers should look into.[65] Since at least 2008, scholars have proposed new agencies to ensure algorithmic fairness and accountability.[66] Some researchers argue for a "watchdog system that allows users to detect discriminatory practices."[67] Joanna Bryson has proposed that "Citizens (or perhaps citizens' advocates, see next paragraph) should be able to trigger audits of software systems when they suspect conditions such as a) the inappropriate or unauthorized use of data, or b) unfair or unlawful bias."[68] Whatever the details, one thing is clear: algorithmic "pricing may require new approaches to competition investigations, and possibly even to the legal definition of competition infringements," as well as

---

it is nearly impossible for respondents to know what personal or behavioral information may have factored into an unfavorable outcome.").

[64] Jerry Useem, How Online Shopping Makes Suckers of Us All, *The Atlantic* (May 2017), https://www.theatlantic.com/magazine/archive/2017/05/how-online-shopping-makes-suckers-of-us-all/521448/.

[65] Jędrzej Niklas, The regulatory future of algorithms, at http://blogs.lse.ac.uk/mediapolicyproject/2017/08/15/the-regulatory-future-of-algorithms/.

[66] Oren Bracha & Frank Pasquale, Federal Search Commission? Access, Fairness, And Accountability in the Law of Search, at http://www.lawschool.cornell.edu/research/cornell-law-review/upload/Bracha-Pasquale-Final.pdf; Andrew Tutt, An FDA for Algorithms, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2747994; Ryan Calo, The case for a federal robotics commission, at https://www.brookings.edu/research/the-case-for-a-federal-robotics-commission/.

[67] Jakub Mikians, Laszlo Gyarmati, Vijay Erramelli & Nikolaos Laoutaris, Detecting Price and Search Discrimination on the Internet, 2012 Proc. 11th ACM Workshop On Hot Topics Networks 79, at http://www.ccs.neu.edu/home/cbw/static/class/5750/papers/hotnets2012_pd_cr.pdf.

[68] Bryson, Testimony for the The House of Lords Select Committee on Artificial Intelligence, at https://joanna-bryson.blogspot.com/2017/09/testimony-for-the-house-of-lords-select.html.

new consumer protections.[69] As Rick Swedloff has argued, "while big data may be a natural next step in risk classification, it may require a revolutionary approach to regulation."[70]

3) How effective are current policies and communications with consumers regarding the collection and use of personal data?

Current policies are failing because, when it comes to consumers' relationships with dominant providers, they are based on a category mistake. Online "terms of service" are not ordinary contracts. They cannot be negotiated or otherwise altered. They are take-it-or-leave it deals offered by must-have services.[71] Thus privacy policies are experienced, by most, as a form of "privacy theater," and may even be viewed as "exposure policies," since they so often reserve so many rights to data exploitation to the more powerful entity in the so-called bargain.

This category mistake arose out of a naïvely economistic approach to privacy as a normal good or service to be bargained for, like any other. Within a neoclassical economic framework, the relationship between Internet privacy and competition is direct and positive. Consumers set out to obtain an optimal amount of privacy as a feature of the Internet services they consume. Just as a car buyer might choose a Volvo over a Ford because the Volvo is said to have better crash impact protection than the Ford, so too might a search engine user choose DuckDuckGo over Google because of the privacy DuckDuckGo offers.[72] Companies compete to offer more or

[69] Oxera Economic Council, When Algorithms Set Prices: Winners And Losers (2017), at https://www.regulation.org.uk/library/2017-Oxera-When_algorithms_set_prices-winners_and_losers.pdf.
[70] Swedloff, Risk Classification's Big Data (R)evolution, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2566594 (2014).
[71] The rest of this section is drawn from Frank Pasquale, *Privacy, Antitrust, and Power,* George Mason L. Rev. (2013).
[72] Google's advocates frequently mention DuckDuckGo as a competitor, but industry experts are skeptical. Brooke Gladstone, *Can a Small Search Engine Take on Google?,* ON THE MEDIA, at http://www.onthemedia.org/2013/apr/12/duck-duck-go-and-competition-search-market/transcript/, Apr.

less privacy to users. If there are many companies in a given field, they will probably offer many different levels of privacy to consumers. If consumers choose to use services from companies that offer little to no privacy protection, that reveals a preference to spend little to nothing on (or looking for) privacy.

Within the neoclassical model, there is little reason for government to limit a firm's collection, analysis, and use of data. Consumers individually decide how much information they want to release about themselves into commercial ecosystems. Indeed, such limits might even undermine the competition that is supposed to be the primary provider of privacy.[73] Companies may need to share data with one another in order to compete effectively. Privacy laws that interfere with that sharing press firms to merge, so that they can seamlessly utilize data that they would have sold or traded to one another in the absence of privacy laws restricting that action.

It would be nice to believe that market forces are in fact promoting optimal levels of privacy. It would also be comforting if antitrust law indirectly promoted optimal privacy options by assuring a diverse range of firms that can compete to supply privacy at various levels (and in

---

12, 2013 ("DuckDuckGo doesn't collect any of your personal data, at all, full stop. . . . Still, Danny Sullivan, who founded Search Engine Land.com, laughed when Google cited DuckDuckGo as a contender. 'It would be like a major baseball player saying, yeah, there's plenty of great athletes out there, look at this kid who's in eighth grade. And the only reason it can really get counted is because there's relatively little competition in the space . . . .'" [said Sullivan].). Sullivan's points here were prophetic, and likely only to become more so.

[73] Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 NW. U. L. REV. COLLOQUY 1, 11–12 (2008) ("An uneven playing field that allows one firm to use the information that it sees while blocking others from doing the same thing creates market power through limiting competition. We rarely want to do that. And privacy rules that limit how information can be used and shared across firms will artificially push towards greater consolidation, something that usually works against maintaining robust competition."). Picker argued that privacy laws restricting interfirm (but not intrafirm) data-sharing may actually undermine competition by encouraging consolidation of firms..

various forms).[74] But this position is not remotely plausible. Antitrust law has been slow to recognize privacy as a dimension of product quality, and the competition that antitrust promotes can do as much to trample privacy as to protect it.[75] In an era of big data, every business has an incentive to be nosy in order to maximize profits.[76]

This account of "competition promoting privacy" only achieves surface plausibility by privileging the short-term "preferences" of consumers to avoid data sharing.[77] The narrowness of "notice-and-consent" as a privacy model nicely matches the short-term economic models now dominating American antitrust law. The establishment in the field is largely unconcerned with too-big-to-fail banks, near monopoly in search advertising, media consolidation, and other forms of industrial concentration. By focusing myopically on efficiency gains that can be temporary or exaggerated, they gloss over the long term pathologies of corporate concentration.[78] So, too, does a notice-and-consent privacy regime privilege on-the-fly, snap judgments of consumers to

[74] "Indirectly" is used here because it is now antitrust orthodoxy that this field of law exists only to protect competition, not competitors, and therefore is concerned first and foremost with *directly promoting consumer welfare.* For an account of the rise of consumer welfare as antitrust's standard (and the problems this has caused), *see* Barak Orbach, *How Antitrust Lost Its Goal*, 81 FORDHAM L. REV. 2253, 2253 (2013) ("while 'consumer welfare' was offered as a remedy for reconciling contradictions and inconsistencies in antitrust, the adoption of the consumer welfare standard sparked an enduring controversy, causing confusion and doctrinal uncertainty.").

[75] As Paul Ohm has documented, competition among broadband ISPs has led them to "search for new sources of revenue . . . [by] 'trading user secrets for cash,' which Google has proved can be a very lucrative market." Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1420 (2009) (describing the many commercial pressures leading carriers to "monetize[] behavioral data at the expense of user privacy").

[76] VIKTOR-MAYER SCHONBERGER AND VICTOR CUKIER, BIG DATA (2013).

[77] Even if consumers tried to opt out more often, notice-and-consent is increasingly irrelevant because, in an era of big data, whatever one might try to hide by keeping certain pieces of data private is increasingly easy to infer from other pieces of data. *Id.*

[78] For a critique of contemporary antitrust, *see* BARRY C. LYNN, CORNERED: THE NEW MONOPOLY CAPITALISM AND THE ECONOMICS OF DESTRUCTION 30 (2010) ("superconsolidation is pretty much standard operating procedure for all industries in the United States these days."); Frank Pasquale, *When Antitrust Becomes Protrust*, at https://www.competitionpolicyinternational.com/wp-content/uploads/2017/05/CPI-Pasquale.pdf.

"opt-in" to one-sided contracts, over a reflective consideration of how data flows might be optimized for consumers' interests generally. As privacy declines and companies consolidate, mainstream antitrust and privacy theory often legitimates the process. Some scholarship can even amount to the "structural production of ignorance," characterizing scenarios as "consent" and "competition" when they are experienced by consumers and users as coercive and monopolistic.[79]

In response to these problems, many advocates have called for more transparency. Privacy regulators should also require auditors to gain a deep understanding of data broker practices, so they can quickly detect and deter failures to adhere to data collection, labeling, and filtering standards. The key here is to begin separating out the many zones of life Big Data grandees are so keen to integrate in databases. Health privacy experts have already spearheaded "data segmentation for privacy" in medical records, allowing for, say, a person to segregate entries from a psychiatrist from those coming from a podiatrist. It is time for the controllers of Big Data generally to become far more careful about how they log data, to be sure its collection, analysis, and use can be influenced by public values, and not just the profit motive.[80]

---

[79] Robert N. Proctor, *Agnotology: A Missing Term to Describe the Cultural Production of Ignorance (and Its Study), in* AGNOTOLOGY: THE MAKING AND UNMAKING OF IGNORANCE 3 (Robert N. Proctor & Londa N. Schiebinger eds., 2008).

[80] Recent rules proposed in New York in the wake of the Equifax scandal may also be of use here. See https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/DFS_CRA_Reg.pdf#_blank; see generally *Written Testimony of Frank Pasquale Before the United States Senate Committee on Banking, Housing, and Urban Affairs*, "Exploring the Fintech Landscape," at https://www.banking.senate.gov/public/_cache/files/0a92ad09-6834-4d7e-901a-6ae5c51572ae/6F5BB3DB26E6C8891F7A5627A3678DCE.pasquale-testimony-9-12-17.pdf; *Testimony and Statement for the Record of Marc Rotenberg, Hearing on Consumer Data Security and the Credit Bureaus Before the Committee on Banking, Housing, and Urban Affairs of the United States Senate*, at https://www.banking.senate.gov/public/_cache/files/19fa71b4-224a-4331-aec7-2fc99081e383/FF627C28C101D75E809511A6D36B284B.rotenberg-testimony-10-17-17.pdf.

4) Conclusion

I have painted a bleak picture of big data and algorithms in this testimony. However, there is good news on the horizon. Over the past decade, a number of visionaries have developed a movement for accountability by the users of algorithms.[81] It took a combination of computational, legal, and social scientific skills to unearth each of the examples discussed above – troubling collection, bad or biased analysis, and discriminatory use.[82] Empiricists may be frustrated by the 'black box' nature of algorithmic decision-making; they can work with legal scholars and activists to open up certain aspects of it (via freedom of information and fair data practices). Journalists, too, have been teaming up with computer programmers and social scientists to expose new privacy-violating technologies of data collection, analysis, and use – and to push regulators to crack down on the worst offenders.

Researchers are going beyond the analysis of extant data, and joining coalitions of watchdogs, archivists, open data activists, and public interest attorneys, to assure a more balanced set of 'raw materials' for analysis, synthesis, and critique. Social scientists and others must commit to the vital, long term project of assuring that algorithms are producing fair and relevant documentation; otherwise large internet firms, states, banks, insurance companies and other powerful actors will make and own more and more inaccessible data about society and people. Algorithmic accountability is a big tent project, requiring the skills of theorists and practitioners, lawyers, social scientists, journalists and others. It's an urgent, global cause with

[81] Groups like AINow, Data & Society, Data for Black Lives, and many others are part of this trend. Early scholarly work included Lucas Introna & Helen Nissenbaum, *Shaping the Web: Why the Politics of Search Engines Matters* (2000), at https://www.nyu.edu/projects/nissenbaum/papers/ShapingTheWeb.pdf.

[82] This section is largely drawn from Frank Pasquale, Digital Star Chamber, at https://aeon.co/essays/judge-jury-and-executioner-the-unaccountable-algorithm.

committed and mobilized experts looking for support. Lawmakers can help by, for example, requiring openness in algorithm used in many governmental contexts.[83]

The world is full of algorithmically driven decisions. One errant or discriminatory piece of information can wreck someone's employment or credit prospects. It is vital that citizens be empowered to see and regulate the digital dossiers of business giants and government agencies.[84] Even if one believes that no information should be 'deleted' – that every slip and mistake anyone makes should be on a permanent record for ever – that still leaves important decisions to be made about the processing of the data. Algorithms can be made more accountable, respecting rights of fairness and dignity for which generations have fought. The challenge is not technical, but political, and the first step is law that empowers people to see and challenge what algorithms are saying about us.

---

[83] See, e.g., the proposal *A Local Law to amend the administrative code of the city of New York, in relation to automated processing of data for the purposes of targeting services, penalties, or policing to persons*, at http://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0&Options=&Search=; Alex Campolo, Madelyn Sanfilippo, Meredith Whittaker, and Kate Crawford, *AINow 2017 Report* ("Core public agencies, such as those responsible for criminal justice, healthcare, welfare, and education (e.g "high stakes" domains) should no longer use "black box" AI and algorithmic systems"). I expect many of these algorithms to undergo increasing scrutiny in coming years. See, e.g., Virginia Eubanks, *Automated Inequality* (forthcoming, 2018).

[84] European data protection law should provide some inspiration for US policymakers as well here. See, e.g., Andrew D. Selbst and Julia Powles, *Meaningful Information and the Right to Explanation*, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3039125; Gianclaudio Malgieri Giovanni Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, at https://academic.oup.com/idpl/advance-article-abstract/doi/10.1093/idpl/ipx019/4626991. For background on the development of "explainable AI," see Cliff Kuang, *Can an AI Be Taught to Explain Itself?*, at https://www.nytimes.com/2017/11/21/magazine/can-ai-be-taught-to-explain-itself.html. Policymakers should try to channel the development of AI that ranks, rates, or sorts humans, toward explainable (rather than black box) models.