



February 15, 2019

Federal Trade Commission
Office of the Secretary
Constitution Center
400 7th Street SW
Washington, DC 20024

Re: Post-Hearing Comments on Algorithms, Artificial Intelligence, and Predictive Analytics for the Federal Trade Commission's Hearings on Competition and Consumer Protection in the 21st Century on November 13-14, 2018, FTC-2018-0101

Dear Sir or Madam:

Consumer Reports¹ writes to submit comments on the hearing and questions posed following the Federal Trade Commission's (FTC or Commission) November 13-14, 2018 hearing on algorithms, artificial intelligence, and predictive analytics.

Questions

Background on Algorithms, Artificial Intelligence, and Predictive Analytics, and Applications of the Technologies

1. What features distinguish products or services that use algorithms, artificial intelligence, or predictive analytics? In which industries or business sectors are they most prevalent?
2. What factors have facilitated the development or advancement of these technologies? What types of resources were involved (e.g., human capital, financial, other)?
3. Are there factors that have impeded the development of these technologies? Are there factors that could impede further development of these technologies?

¹ Consumer Reports is an expert, independent, nonprofit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. As the world's largest independent product-testing organization, it conducts its policy and mobilization work in the areas of privacy, telecommunications, financial services, food and product safety, and other areas. Using its dozens of labs, auto test center, and survey research department, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 7 million members and publishes its magazine, website, and other publications.

4. What are the advantages and disadvantages for consumers and for businesses of utilizing products or services facilitated by algorithms, artificial intelligence, or predictive analytics?
5. From a technical perspective, is it sometimes impossible to ascertain the basis for a result produced by these technologies? If so, what concerns does this raise?

As we note below in response to question 9, in some cases, algorithms are programmed to learn or evolve over time, such that a developer might not know why certain inputs lead to certain results. This could lead to unfair results if there is no meaningful accountability for how decisions are made. If an algorithm is (1) used for a purpose that is likely to have substantial effects on the individual, like the determination of a credit score² and (2) its outcomes cannot be sufficiently explained, then the process should not be used. The FTC and other appropriate regulatory bodies must establish a process for determining what constitutes sufficient explanation and testability, and must also establish standards to protect against harm, including harms not covered by existing laws that may emerge over time.

6. What are the advantages and disadvantages of developing technologies for which the basis for the results can or cannot be determined? What criteria should determine when a “black box” system is acceptable, or when a result should be explainable?

As we note below in response to question 9, algorithmic transparency is an integral piece of any algorithmic accountability framework. In addition, if an algorithm is used for a significant purpose, such as the determination of a credit score or an assessment of recidivism risk,³ and the algorithm and its outcome cannot be sufficiently explained, then the algorithm should not be used to assess the issue at hand. Significant purposes should include, but not limited to: (1) employment, (2) credit scores and other assessments of credit worthiness, (3) law enforcement, and (4) housing.

Common Principles and Ethics in the Development and Use of Algorithms, Artificial Intelligence, and Predictive Analytics

7. What are the main ethical issues (e.g., susceptibility to bias) associated with these technologies? How are the relevant affected parties (e.g., technologists, the business

² BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION?, FED. TRADE COMM’N (Jan. 2016), *available at* <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>. For this reason, the Fair Credit Reporting Act requires explainability today for credit determinations. However, other important determinations not covered by FCRA may be completely unregulated.

³ Karen Hao, *AI is Sending People to Jail—and Getting it Wrong*, MIT TECH REV. (Jan. 21, 2019), <https://www.technologyreview.com/s/612775/algorithms-criminal-justice-ai/>.

community, government, consumer groups, etc.) proposing to address these ethical issues? What challenges might arise in addressing them?

8. Are there ethical concerns raised by these technologies that are not also raised by traditional computer programming techniques or by human decision-making? Are the concerns raised by these technologies greater or less than those of traditional computer programming or human decision-making? Why or why not?
9. Is industry self-regulation and government enforcement of existing laws sufficient to address concerns, or are new laws or regulations necessary?

Industry self-regulation and government enforcement of existing laws are not sufficient to address consumers' concerns about the use of these new and emerging tools. Algorithms are increasingly being used to make life-impacting decisions (especially in employment decisions and in the criminal justice system), but they lack requisite auditing and accountability for their use. The vast majority of algorithmic decision-making is currently unregulated, not subject to any federal law. The United States lacks any federal laws that speak directly to the issues that the use of algorithms by government entities or by private actors pose; however, there are sector-specific laws that ban discrimination on the basis of race, sex, religion, and other traits in the areas of housing,⁴ employment,⁵ and credit.⁶ Although New York city passed a law that creates a task force designed to give recommendations to the state regarding use of algorithms by state agencies,⁷ this task force lacks any additional power to hold algorithms accountable. It is scheduled to release its report in late 2019.

We also lack sufficient technical safeguards for the use of algorithmic decision-making tools. While researchers have discovered several discriminatory effects noted above, in fact few algorithms and other scoring systems have been scientifically assessed. The risks of using algorithms to make important decisions about individuals are exacerbated by the flawed assumption that algorithms are scientific and inherently neutral:

Their popularity relies on the notion they are objective, but the algorithms that power the data economy are based on choices made by fallible human beings.

⁴ FAIR HOUSING ACT, 42 U.S.C. § 3604(a), (f).

⁵ TITLE VII OF THE CIVIL RIGHTS ACT OF 1964, 42 U.S.C. § 2000e-2(a)-(b); AGE DISCRIMINATION IN EMPLOYMENT ACT, 29 U.S.C. § 623(a); 29 U.S.C. § 623(e); AMERICANS WITH DISABILITIES ACT, 42 U.S.C. § 12112(a); and GENETIC INFORMATION NONDISCRIMINATION ACT, 42 U.S.C. § 2000ff et seq.

⁶ EQUAL CREDIT OPPORTUNITY ACT, 15 U.S.C. § 1691(a). The Fair Housing Act applies to the issuing of mortgage loans. 42 U.S.C. § 3605(a)

⁷ The law creates a task force that provides recommendations on how information on agency automated decision systems may be shared with the public and how agencies may address instances where people are harmed by agency automated decision systems. *A Local Law in Relation to Automated Decision Systems Used by Agencies, Int. 1696*, N.Y. CITY COUNCIL (2017), available at <http://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0>.

And, while some of them were made with good intentions, the algorithms encode human prejudice, misunderstanding, and bias into automatic systems that increasingly manage our lives. Like gods, these mathematical models are opaque, their workings invisible to all but the highest priests in their domain: mathematicians and computer scientists. Their verdicts, even when wrong or harmful, are beyond dispute or appeal. And they tend to punish the poor and the oppressed in our society, while making the rich richer.

Finally, consumers also lack any means to correct erroneous conclusions made by algorithms, or any recourse to object to the use of an untested and undisclosed algorithm to make inferences or decisions about them.

We urge the FTC to give guidance directing companies and organizations that use algorithms to do regular assessments of the accuracy of the algorithmic decisions, and to inspect the source code in order to root out any inherent or sample-bias that has been embedded in the algorithm.

Algorithms are used widely, without any accountability or consumer knowledge and control over their use, to make important, and sometimes life-changing, decisions about individuals. In order for consumers to be sufficiently protected, the FTC needs, and should request, additional authority and resources to assess the use of algorithms and to require companies to provide easy means for correction of consumer data that is used in the algorithm. The Commission's authority should also include the ability to create rules requiring audits of algorithms and mandating in some cases some right of redress and human intervention. In the meantime, the Commission should craft guidelines for the use of algorithms to help determine whether a particular algorithm produces decisions that are fair, accurate and representative. To that end, any guidance, at a minimum, should include the following principles:

- **The use of algorithms should be transparent to the end users.** When algorithms make decisions about consumers the individual should have notice that an algorithm was used. In many cases, such as in the sorting of posts in a social media feed or in the prioritization of search results, this will be obvious and no dedicated notice will be necessary; but in some non-intuitive settings, companies should let consumers know when some decision-making relies on algorithmic evaluation.
- **Algorithmic decision-making should be testable for errors and bias, while still preserving intellectual property rights.** Algorithms should be able to be tested by outside researchers and investigators.⁹ Opaque algorithms that have the ability to affect a

⁸ Cathy O'Neil, *How Algorithms Rule Our Working Lives*, THE GUARDIAN (Sept. 1, 2016), <https://www.theguardian.com/science/2016/sep/01/how-algorithms-rule-our-working-lives>.

⁹ See, e.g., Lauren Kirchner, *Federal Judge Unseals New York Crime Lab's Software for Analyzing DNA Evidence*, PROPUBLICA (Oct. 20, 2017), <https://www.propublica.org/article/federal-judge-unseals-new-york-crime-labs-software-for-analyzing-dna-evidence>

large number of people in life-changing ways should be subject to higher scrutiny. Using this assessment, algorithms used in life-altering situations, such as the employment process and in the creation of FICO and similar scores, warrant greater scrutiny.

Currently, the US lags behind on algorithmic transparency compared to our European counterparts.¹² The European Union incorporated algorithmic transparency and accountability into their new data privacy law: any decision based “solely on automated processing” which includes “legal effects” or “similarly significantly affects” an individual, be subject to “suitable safeguards,” including an opportunity to obtain an explanation of an algorithmic decision, and to challenge such decisions.” France’s president, Emmanuel Macron, pledged that the country will make all algorithms used by its governments open to the public. And in June, the United Kingdom called for public sector entities to be transparent and accountable about their data practices and to “carefully consider the social implications of the data and algorithms used.”

- **Algorithms should be designed with fairness and accuracy in mind.** Companies should not simply rely on outsiders to detect problems with their algorithms; instead, companies should be required to plan for and design to avoid adverse consequences at all stages of the development of algorithms. Algorithms based on current data sets should be examined closely at the design stage in order to weed out historic discriminatory attitudes. Algorithms can “inherit the prejudices of prior decision makers...in other

¹⁰ CATHY O’NEIL, *WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY*, p. 152 (2016) [hereinafter *WEAPONS OF MATH DESTRUCTION*].

¹¹ Algorithms are used in state and local agencies across the country, including Arkansas: “Algorithmic tools like the one Arkansas instituted in 2016 are everywhere from health care to law enforcement, altering the ways people affected can usually only glimpse, if they know they’re being used at all. Even if the details of algorithms are accessible, which isn’t always the case, they’re often beyond the understanding of the people using them, raising questions about what transparency means in an automated age, and concerns about people’s ability to contest decisions made by machines.” Colin Lecher, *What Happens When an Algorithm Cuts Your Health Care*, *THE VERGE* (Mar. 21, 2018), <https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy>. The article describes similar algorithmic tools used in other states, including California, Colorado, and Idaho. *See, also*, Alvin Roth, *Why New York City’s High School Admissions Process Only Works Most of the Time*, *CHALKBEAT* (July 2, 2015), <https://www.chalkbeat.org/posts/ny/2015/07/02/why-new-york-citys-high-school-admissions-process-only-works-most-of-the-time/>; *and*, NORTH CAROLINA GOVERNMENT DATA ANALYTICS CENTER, *NC IT*, <https://it.nc.gov/services/nc-gdac> (last visited Aug. 17, 2018).

¹² Julia Angwin, *Making Algorithms Accountable*, *PROPUBLICA* (Aug. 1, 2016), <https://www.propublica.org/article/making-algorithms-accountable>.

¹³ Art. 22, *GENERAL DATA PRIVACY REGULATION*, <https://gdpr-info.eu/art-22-gdpr/>.

¹⁴ Nicholas Thompson, *Emmanuel Macron Talks to Wired about France’s AI Strategy*, *WIRED* (Mar. 31, 2018), <https://www.wired.com/story/emmanuel-macron-talks-to-wired-about-frances-ai-strategy/>.

¹⁵ *Data Ethics Framework*, UK DEP’T FOR DIGITAL, CULTURE, MEDIA & Sport (June 13, 2018), <https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework>.

¹⁶ The use of algorithms in the criminal justice sector sufficiently demonstrates the perils of using existing data sets

cases, data may simply reflect the biases that persist in society at large.” To correct for sample size disparity that would disproportionately favor the creators or the majority of the data-set population, the data sets used in the algorithmic tool should be thoroughly assessed to root out any unintended bias towards any group.¹⁸ Since algorithms and all data-driven products “will always reflect the design choices of the humans who built them,” companies should commit to the further diversification of their employees.

- **The data set used for algorithmic decision-making should avoid the use of proxies.** Algorithms can only serve to address the question posed to it. When possible, algorithms should avoid the use of unnecessary proxies like zip codes or credit scores that may be used to make discriminatory decisions against individuals. This problem persists even when the creators are trying to correct for unexpectedly biased results: “Even in situations where data miners are extremely careful, they can still [e]ffect discriminatory results with models that, quite unintentionally, pick out proxy variables for protected classes.” For instance, a joint collaboration between Consumer Reports and ProPublica demonstrated that car insurance companies were using an individual’s zip code as a proxy for race and class in order to discriminatorily charge customers in minority-majority neighborhoods a higher price for car insurance.²²

to evaluate problems in a new way. “Our analysis of Northpointe’s tool, called COMPAS [...] found that black defendants were far more likely than white defendants to be incorrectly judged to be at a higher rate of recidivism, while white defendants were more likely than black defendants to be incorrectly flagged as low risk[...]even when controlling for prior crimes.” Jeff Larson, *et al.*, *How We Analyzed the COMPAS Recidivism Algorithm*, PROPUBLICA (May 23, 2016), <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>. The risk assessment used by Northpointe was based on data that included items that can be correlated with race, such as poverty, joblessness, and social marginalization. Judges have used these scores in their sentencing decisions, despite the exacerbation of bias that the algorithm created. This algorithm, that was used to decide many individuals’ fates, was not rigorously tested before use: “As often happens with risk assessment tools, many jurisdictions have adopted Northpointe’s software before rigorously testing whether it works.” Julia Angwin & Jeff Larson, *Machine Bias*, PROPUBLICA (May 23, 2016), <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

¹⁷ Solon Barocas & Andrew D. Selbst, *Big Data’s Disparate Impact*, 104 CALIF. LAW REV. 671 (2016), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899.

¹⁸ Organizations can available tools to test whether algorithms already in use and algorithms in the design stage have a discriminatory effect. Researchers are actively developing tools they hope companies and government agencies could use to test whether their algorithms yield discriminatory results and to fix them when necessary. *See, e.g., Utah Computer Scientists Discover How to Find Bias in Algorithms*, UNIV. OF UTAH (Aug. 14, 2015), <https://unews.utah.edu/programming-and-prejudice/>. Cathy O’Neil also created a company that audits algorithms to see how biased they are. *See O’NEIL RISK CONSULTING & ALGORITHMIC AUDITING*, <http://www.oneilrisk.com/> (last visited Aug. 17, 2018).

¹⁹ Nanette Byrnes, *Why We Should Expect Algorithms to be Biased*, MIT TECH. REV. (June 24, 2016), <https://www.technologyreview.com/s/601775/why-we-should-expect-algorithms-to-be-biased/>.

²⁰ *See, e.g.,* Nitasha Tiku, *Google’s Diversity Stats are Still Very Dismal*, WIRED (June 14, 2018), <https://www.wired.com/story/googles-employee-diversity-numbers-havent-really-improved/>.

²¹ *Big Data’s Disparate Impact*, *supra* note 17; Karen Levy & danah boyd, *Networked Rights and Networked Harms*, paper presented at the INT’L COMMC’N ASSOC.’S DATA & DISCRIMINATION PRECONFERENCE (May 14, 2014), <http://www.datasociety.net/initiatives/privacyand-harm-in-a-networked-society/>.

²² *Auto Insurers Charging Higher Rates in Some Minority Neighborhoods*, CONSUMER REPORTS (Apr. 4, 2017),

- **Algorithmic decision-making processes that could have significant consumer consequences should be explainable.** In some cases, algorithms are programmed to learn or evolve over time, such that a developer might not know why certain inputs lead to certain results. This could lead to unfair results if there is no meaningful accountability for how decisions are made. If an algorithm is (1) used for a significant purpose, like the determination of a credit score²³ and (2) cannot be sufficiently explained, then the process should not be used.

Consumer Protection Issues Related to Algorithms, Artificial Intelligence, and Predictive Analytics

11. What are the main consumer protection issues raised by algorithms, artificial intelligence, and predictive analytics?
12. How well do the FTC’s current enforcement tools, including the FTC Act, the Fair Credit Reporting Act, and the Equal Credit Opportunity Act, address issues raised by these technologies?

Deception

The FTC has substantial—though insufficient—tools to address algorithmic processing and artificial intelligence; however, a dated and narrow interpretation of *deception* unnecessarily constrains its existing tools: the Deception Policy Statement should be updated to reflect policy concerns in a world increasingly intermediated by algorithms and code. Today, under the Deception Policy Statement,²⁴ in order to be considered deceptive, a “representation, omission, or practice must be likely to mislead *reasonable consumers* under the circumstances.”²⁵ This requirement that a consumer is directly misled incorrectly excludes a wide range of deceptive and harmful behavior—a range of behavior that is only going to increase as AI advances. The Deception Policy Statement should be revised and expanded to include at least (a) deception of software-based user agents acting on a consumer’s behalf and (b) deception of independent testers, regulators, or evaluators of consumer services. More broadly, deceiving AI working on behalf of consumers — or the use of malicious AI trying to evade accountability — should be considered within the ambit of the FTC’s deception authority.

https://www.consumerreports.org/media-room/press-releases/2017/04/propublica_and_consumer_reports_auto_insurers_charging_higher_rates_in_some_minority_neighborhoods11/.

²³ BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION?, *supra* note 2. For this reason, the Fair Credit Reporting Act requires explainability today for credit determinations. However, other important determinations not covered by FCRA may be completely unregulated.

²⁴ *Policy Statement on Deception*, FED. TRADE COMM’N (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

²⁵ *Id.*

Historically, the FTC has failed to take action against companies that evade another company's software acting on behalf of a user. For example, in 2011, it was reported that Amazon circumvented Internet Explorer settings that provided preferential treatment to companies that disclosed privacy practices in a short-form privacy policy (known as P3P).²⁶ Rather than provide structured information in the prescribed P3P format, Amazon's policy simply contained the gibberish "AMZN," essentially allowing it to trick Internet Explorer into more favorable treatment of Amazon's cookies. The FTC failed to bring an enforcement action against Amazon, even though its behavior was certainly *deceptive*, which led to Amazon having a greater capacity to track users.

Similarly, in 2012, the FTC failed to charge that Google's practice of evading Apple Safari's browser controls limiting third-party cookies was a deceptive practice under Section 5. Although the FTC did bring an enforcement action, its case was predicated consumer-facing statements in an FAQ on its site stating that Google lacked the ability to track Safari users.²⁷ However, the case would have been stronger and established a more important precedent if it had challenged the underlying practice of circumventing Apple's privacy controls instead. Notably, the parallel multi-state Attorney General action against Google did target the underlying practice and was not predicated entirely on the deceptive statement on Google's consumer-facing statements.²⁸

Tricking or evading computerized systems will only be more of a consumer protection problem as consumers rely more on software and artificial intelligence to act on their behalf. A shopping tool, for example, that is designed to reorder contact lenses from the cheapest source every six months should not be thwarted by tricks to hide competitors' prices or obscure add-on fees that would affect overall cost. Certain search engine optimization, intellectual property takedown requests, or social media amplification tactics might also be reasonably and beneficially prohibited by a more comprehensive definition of deception. Artificial intelligence has the potential to be extremely useful for consumers, but as we heard at the FTC's public workshop, it also tends to be brittle and susceptible to gaming. The FTC should enunciate clear

²⁶ Chris Morran, *Amazon Sued Over Alleged Privacy Policy Violations*, CONSUMERIST (Mar. 4, 2011), <https://consumerist.com/2011/03/04/amazon-sued-over-invasion-of-privacy-allegations/>.

²⁷ Press Release, Google Will Pay \$22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser, FED. TRADE COMM'N (Aug. 9, 2012), <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented>. The complaint also alleged that consumer-facing statements asserting compliance with industry self-regulatory standards were deceptive as well.

²⁸ Press Release, A.G. Schneiderman Announces \$17 Million Multistate Settlement With Google Over Tracking Of Consumers, OFFICE OF THE NY ATT. GEN. (Nov. 18, 2013), <https://ag.ny.gov/press-release/ag-schneiderman-announces-17-million-multistate-settlement-google-over-tracking>.

policies and bring enforcement action to establish policy backstops to prevent the manipulation of software systems in ways that disadvantages consumers.

In addition to expanding its concept of deception to encompass deception toward software and AI acting on a consumer's behalf, the FTC should also make clear that the use of software or AI to deceive non-consumer regulator, testing, or evaluation services (such as Consumer Reports) constitutes a deceptive practice. Although these services are not typically the intended end user of most consumer products, they provide an essential value to the marketplace in providing information and uprooting bad or illegal behavior. As such, the Deception Policy Statement should be modernized to include deceptive practices aimed at these entities that disadvantages consumers.

For example, in 2016, the Federal Trade Commission charged Volkswagen with deceptive practices over “defeat devices” designed to circumvent emissions testing programs.²⁹ Again, however, the FTC relied upon public facing statements to consumers that the cars used “clean diesel” technologies or were environmentally friendly — not that Volkswagen's cars were configured to provide misleading data to evaluating systems in testing environments. Consider instead if Volkswagen had never made any statements about, say, gas mileage but used similar tricks to fool regulators' systems into believing (and later publishing) that Volkswagen diesel cars achieved better mileage than in fact consumers could expect (or that they were in compliance with minimum statutory requirements). That type of deception should also be considered within the scope of Section 5 as it clearly harms consumers and frustrates informed market choices.

Similarly, the use of software to provide inaccurate or misleading results to independent testing labs such as Consumer Reports should also be considered a deceptive practice under Section 5. Every year, Consumer Reports tests thousands of products in our lab for our magazine, website, and app for our seven million members. If a company were able to detect that it was being tested in our labs (connected and smart products may have a far greater capacity to this), it could change its behavior to manipulate our tests, leading to inaccurate information being provided to the marketplace. In the past, for example, chipset manufacturers have been accused of detecting when laboratories were likely to be performing industry benchmarking tests, and changing their behavior to game those tests (performing at elevated speeds that would be impossible or impractical to achieve over an extended period of time).³⁰ However, no regulator

²⁹ Press Release, FTC Charges Volkswagen Deceived Consumers with Its “Clean Diesel” Campaign, FED. TRADE COMM'N (Mar. 29, 2016), <https://www.ftc.gov/news-events/press-releases/2016/03/ftc-charges-volkswagen-deceived-consumers-its-clean-diesel>.

³⁰ Jacob Siegal, Galaxy Note 3 juices benchmark tests, Phil Schiller takes note, BGR (Oct. 1, 2013), <https://bgr.com/2013/10/01/galaxy-note-3-benchmarks-rigged/>.

brought an enforcement action against this behavior. In an era increasingly dominated by algorithmic and AI systems, companies should probably be *required* to enable third-party testing to ensure meaningful accountability; certainly, however, efforts to *affirmatively mislead* third-party testing services should be prohibited.

(On a related note, contrary to the suggestion of at least one former Commissioner,³¹ the FTC should continue to deem that false statements in privacy policies are material and actionable — even if few consumers themselves actually read them. In evaluating products and services under the Digital Standard,³² Consumer Reports, in part, relies upon company’s policy statements in providing normative assessments of corporate practices; if companies were allowed to lie with impunity in privacy policies, we would be frustrated in our ability to provide meaningful distillations of these policies to consumers in order to empower them to make informed choices.)

Substantiation

The FTC should also issue clarifying guidance and take appropriate enforcement action on *unsubstantiated* and unsupported assertions of AI’s capabilities. Just as many security companies’ representations about “military-grade encryption” and “NSA-proof technology” may veer beyond mere puffery into outright deception, so too might aspirational and evidence-free claims an AI product that is about as effective as snake oil.

For instance, in recent weeks, the Washington Post reported on Predictim, a company that purported to use artificial intelligence to provide a “risk rating” of prospective nannies on separate factors such as “bullying and harassment” and “drug abuse.”³³ The company promoted its technology as “Perfected and Proven Using More Than 6 Billion Data Points,” and sought to scare parents with anecdotes of abusive babysitters, stating “had the parents of the little girl injured by this babysitter been able to use Predictim as part of their vetting process, they would never have left her alone with their precious child.” Nevertheless, based on a review of the service, it is doubtful that Predictim’s technology had been scientifically demonstrated to be fair and accurate. In response to press reports, the company ceased operations in December.

³¹ Dissenting Statement of Commissioner Joshua D. Wright In the Matter of Nomi Technologies, Inc., FED. TRADE COMM’N (Apr. 23, 2015), <https://www.ftc.gov/public-statements/2015/04/dissenting-statement-commissioner-joshua-d-wright-matter-nomi-technologies>.

³² The Digital Standard, <https://www.thedigitalstandard.org/>.

³³ Drew Harwell, *Wanted: The ‘Perfect Babysitter.’ Must Pass AI Scan for Respect and Attitude*, WASH. POST (Nov. 23, 2018), <https://www.washingtonpost.com/technology/2018/11/16/wanted-perfect-babysitter-must-pass-ai-scan-respect-attitude/>.

Indeed, the FTC has in the past brought actions against companies that failed to take reasonable care to ensure that algorithms delivered meaningful and reliable results. In 2012, the FTC brought a wide-ranging case against the data broker Spokeo, including an allegation that the company “failed to use reasonable procedures to assure maximum possible accuracy of consumer report information.”³⁴ Although that case was brought under the Fair Credit Reporting Act, the FTC has in other contexts required substantial evidence to support claims about the effectiveness of products under Section 5.³⁵ Certainly, one can easily imagine other scenarios not covered by FCRA where algorithms overpromise precision (while delivering laughably unreliable accuracy), leading to significant harm for consumers. For example, one service has purported to match uploaded photographs to databases of convicted sex offenders, with dubious results.³⁶ Another company has marketed “voice stress analysis” as a mechanism to identify future criminals,³⁷ asserting “greater than 97% accuracy, [with] no false negatives.”³⁸ Cathy O’Neil’s excellent and compelling book *Weapons of Math Destruction* contains myriad other examples of potentially harmful algorithmic systems not backed up by rigorous science or consumer protection backstops.³⁹ While substantiation of claims about AI and machine-learning may be challenging given that developers themselves often may not fully understand why and when systems are effective, that uncertainty and possible unknowability should not excuse marketers from decades-long precedents of having reasonable evidence of products’ effectiveness.

Manipulation

Finally, it may be worth considering when artificial intelligence might be *too effective* at influencing consumers and coercing behavior. While it may currently be premature to identify where AI-informed advertising may be sufficiently personalized and targeted as to effectively frustrate free choice and autonomy — or exacerbate the widening imbalance of power between companies and consumers — this may be a legitimate concern meriting the Commission’s attention as well as future research. On the other hand, the use of AI and dark patterns to make technology products *addictive* may already be ripe for FTC policy guidance if not enforcement

³⁴ Press Release, Spokeo to Pay \$800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA, FED. TRADE COMM’N (Jun. 12, 2012), <https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed>.

³⁵ *POM Wonderful LLC v. F.T.C.*, 13-1060, __ F.3d __ (D.C. Cir. Jan. 30, 2015).

³⁶ Justin Brookman, Twitter, (Apr. 25, 2014), <https://twitter.com/JustinBrookman/status/459734320697974784>.

³⁷ *How It Works*, AC GLOBAL RISK, <https://www.acglobalrisk.com/how-it-works/> (last visited Feb. 12, 2019).

³⁸ Transcribed conversation from a live broadcast, Alex Martin on Bloomberg Technology News, BLOOMBERG (July 5th, 2018, 5:34 PM ET), https://archive.org/details/BLOOMBERG_20180705_210000_Bloomberg_Technology/start/2040/end/2100 (last visited Feb. 12, 2019); *and, see*, Ava Kofman, *The Dangerous Junk Science of Vocal Risk Assessment*, THE INTERCEPT (Nov. 25, 2018), <https://theintercept.com/2018/11/25/voice-risk-analysis-ac-global>.

³⁹ WEAPONS OF MATH DESTRUCTION, *supra* note 10.

under Section 5 unfairness.⁴⁰ Commercial tactics to maximize consumer engagement at the expense of individual well-being may well present substantial and unavoidable consumer harm that is not offset by countervailing benefits.

13. In recent years, the FTC has held public forums to examine the consumer protection questions raised by artificial intelligence as used in certain contexts (e.g., the 2017 FinTech Forum on artificial intelligence and blockchain and the 2011 Face Facts Forum on facial recognition technology). Since those events, have technological advancements, or the increased prevalence of certain technologies, raised new or increased consumer protection concerns?

The increased use of algorithms, especially as it affects consumers, has certainly led to increased consumer protection concerns. Recent research by Pew since our initial comments demonstrates the following key developments in consumer understanding and exposure to algorithms: (1) “Algorithmically generated content platforms play a prominent role in Americans’ information diet”; (2) “The inner workings of even the most common algorithms can be confusing to users”; (3) “The public is wary of computer algorithms being used to make decisions with real-world consequences”; (4) People’s comfort level with algorithms often depends on how they are used”; (5) “Nearly six-in-ten Americans (58%) think computer programs will always reflect the biases of their designers”; (6) “Algorithm-drive social media platforms can produce feelings of anger in their users — and most Americans are skeptical that the content they see on social media reflects reality”; and (7) “technology experts predict that these systems amplify human autonomy, agency, and capabilities.”⁴¹ Based even on this summary of several nationwide polls (with the exception of point seven which points to a survey of experts), it is clear that consumers lack fundamental transparency controls into how algorithms are used, when they are used, and what affect the algorithm may have. In addition, it is likewise clear that the US population has some understanding that algorithms frequently bake in the biases of their creators and can have deleterious effects on individuals as a result. Consumers are engaged on the issue of algorithms and need effective protections and transparency and use controls that rules from the FTC or a federal law would provide.

While these results do not point to any new concerns that require attention, they do demonstrate that consumers care about the use of algorithms and are worried about the consequences of the use of such tools. Additionally, since algorithms already affect consumers’ social media platforms and what content people taken in, the time is ripe to pass or issue a commonsense

⁴⁰ Ana Homayoun, *Is Your Child a Phone ‘Addict’?*, N.Y. TIMES (Jan. 17, 2018), <https://www.nytimes.com/2018/01/17/well/family/is-your-child-a-phone-addict.html>.

⁴¹ Aaron Smith, *7 Things We’ve Learned About Computer Algorithms*, PEW RESEARCH CTR. Feb. 13, 2019), <http://www.pewresearch.org/fact-tank/2019/02/13/7-things-weve-learned-about-computer-algorithms/>.

consumer protection law or rule that increases transparency and accountability. In addition, these survey results indicate that any protections the FTC or Congress passes on algorithms will have a great effect on consumers.

14. What roles should explainability, risk management, and human control play in the implementation of these technologies?
15. What choices and notice should consumers have regarding the use of these technologies?

Please see our response to question 9, above, for more on this question.

Competition Issues Related to Algorithms, Artificial Intelligence, and Predictive Analytics

17. Does the use of algorithms, artificial intelligence, and predictive analytics currently raise particular antitrust concerns (including, but not limited to, concerns about algorithmic collusion)?

The use of algorithms and other predictive analytics tools raises new antitrust concerns for consumers. Specifically, new research indicates that the use of AI to set online shopping prices may learn to collude. This research shows that “even relatively simple pricing algorithms systematically learned to play sophisticated collusive strategies.” Although this research is relatively new, scholars like Maurice E. Stucke and Ariel Ezrachi warned about the possibility of algorithms to facilitate collusion over two years ago, stating:

Unlike humans, computers do not fear detection, possible financial penalties, or incarceration, and they do not respond in anger. The stability needed for tacit collusion is enhanced by the fact that computer algorithms are unlikely to exhibit other human biases. Human biases can always be reflected in code. But if some biases are minimized (such as loss aversion, the sunk cost fallacy, and framing effects), the algorithm will act more consistently and deliberately than humans in quantifying the profits that are likely achievable through tacit collusion.

⁴² “We show that the propensity to collude is stubborn – substantial collusion continues to prevail even when the active firms are three or four in number, when they are asymmetric, and when they operate in a stochastic environment. The experimental literature with human subjects, by contrast, has consistently found that they are practically unable to coordinate without explicit communication save in the simplest case, with two symmetric agents and no uncertainty.

What is most worrying is that the algorithms leave no trace of concerted action – they learn to collude purely by trial and error, with no prior knowledge of the environment in which they operate, without communicating with one another, and without being specifically designed or instructed to collude. This poses a real challenge for competition policy. While more research is needed before considering policy moves, the antitrust agencies’ call for attention would appear to be well grounded.”

Emilio Calvano, *et al.*, *Artificial Intelligence, Algorithmic Pricing, and Collusion*, VOX EU (Feb. 3, 2019), <https://voxeu.org/article/artificial-intelligence-algorithmic-pricing-and-collusion>.

With the industry-wide use of computer algorithms and the resulting greater transparency of the marketplace, computers can more easily track the behavior of numerous rivals and anticipate and react to competitive threats well before any pricing change. Each firm's algorithm determines whether it can profit by undertaking a competitive initiative. Under our scenarios, the algorithm concludes not. This is because the rivals, possessing the same technology, can quickly identify the competitive initiative and emerging threat and know when and how to retaliate. By responding quickly, the rivals deprive any would-be mavericks of the benefits of launching competitive initiatives, and thereby diminish the incentives to undertake them.

Even more worryingly, these pricing tools “leave no trace of concerted action,”⁴⁴ meaning that pricing algorithms, which are already opaque to the consumer, will not only set prices, but also can work to collude *without a trace*. As we noted in our August 2018 comments to the Commission in advance of the hearings,⁴⁵ pricing algorithms are obscured from the end user by design and information about the use of such pricing algorithms typically “only comes out when there's a leak, when someone from the inside divulges it.” Therefore, this evidence makes pricing algorithms even more unknown and unknowable to the average consumer, who is only offered the price the algorithm sets, even if it is higher based on (possibly inaccurate) assumptions about the consumer and whether or not the price was set at a higher rate thanks to effective algorithmic collusion. And, as the research from Emilio Calvano, et al., shows, Stucke and Ezrachi's warning at the end of the article is now a pressing concern:

We should explore new legal safeguards to promote competition in this new competitive environment. Otherwise, we will likely experience durable forms of collusion that are beyond enforcers' reach, sophisticated forms of price discrimination, and an array of abuses by data-driven monopolies that, by controlling key platforms like smartphone operating systems, can dictate your company's future.

⁴³ Maurice E. Stucke & Ariel Ezrachi, *How Pricing Bots Could Form Cartels and Make Things More Expensive*, HARVARD BUS. REV. (Oct. 27, 2018), <https://hbr.org/2016/10/how-pricing-bots-could-form-cartels-and-make-things-more-expensive>.

⁴⁴ Karen Hao, *Pricing Algorithms Can Learn to Collude With Each Other to Raise Prices*, MIT TECH. REV. (Feb 12, 2019), <https://www.technologyreview.com/the-download/612947/pricing-algorithms-can-learn-to-collude-with-each-other-to-raise-prices/>.

⁴⁵ Justin Brookman & Katie McInnis, *Consumer Protection Comments on the Federal Trade Commission's Announcement of Competition and Consumer Protection in the 21st Century Hearings*, CONSUMER REPORTS (Aug. 21, 2018), <https://advocacy.consumerreports.org/research/consumers-unions-consumer-protection-comments-on-the-federal-trade-commissions-announcement-of-competition-and-consumer-protection-in-the-21st-century-hearings/>.

⁴⁶ Arwa Mahdawi, *Is Your Friend Getting a Cheaper Uber Fare than You Are?*, THE GUARDIAN (Apr. 13, 2019), <https://www.theguardian.com/commentisfree/2018/apr/13/uber-lyft-prices-personalized-data>.

⁴⁷ *How Pricing Bots Could Form Cartels*, *supra* note 43.

Although Stucke and Ezrachi end their admonition with a call for concern about the direction of business, the issues presented in this final caution are prime concerns for consumers who already are feeling the abuses of data-driven monopolies and more advanced methods of price discrimination.

23. How can regulators meet legitimate regulatory goals that may be raised in connection with these technologies without unduly hindering competition or innovation?

In general, the FTC and Congress need to articulate more bright-line rules regarding the use of AI to potentially harm consumers. Although such rules will be necessarily imperfect and imprecise, they are preferable to the alternative: complex, vague, and unenforceable standards. Algorithms and artificial intelligence technologies cannot be solely enforced by frameworks that rely on internal assessments of risk to meaningfully put guardrails around the use of algorithmic processing and AI.

Relatedly, one point that repeatedly came up at the workshop was that the FTC needs more staff — especially technologists.⁵⁰ We strongly agree with this assessment: indeed the agency itself is

⁴⁸ It is extremely difficult for consumers to switch from privacy-invasive platforms to others due to the lack of sufficient competition in the marketplace. First and foremost, in many cases, network effects lock in users to the platforms used by others; absent some sort of mandated interoperability, this is likely to be the case going forward as well. Moreover, the Silicon Valley venture capitalist system is one in which small startups hope for a big buyout from an existing tech giant rather than to become such a giant. In this system, companies can use consumers to spot future competitors (*see, e.g.*, Karissa Bell, *Facebook Used VPN Data to Watch WhatsApp and Snapchat*, MASHABLE (Dec. 5, 2018), <https://mashable.com/article/facebook-used-onavo-vpn-data-to-watch-snapchat-and-whatsapp/>.) and buy out those market challengers before they have the chance to rival platforms like Facebook. Therefore, consumers are effectively prevented from switching to another platform) because those competitors have long been bought out and incorporated into existing companies. The Federal Trade Commission has to date done little to address the anticompetitive effects of these types of prospective acquisitions.

⁴⁹ In our August 2018 comments to the Federal Trade Commission on this subject, we noted that online retailers already use algorithms to create dynamic, individual prices, also known as first-degree price discrimination, on the basis of consumers' assessed willingness to pay and that this price discrimination can lead to a loss of consumer power. When combined with excessive data collection practices and corporate consolidation, companies today have a greater ability to extract a relatively larger amount of consumer surplus for any given transaction. In addition, consumers are also harmed through the use of differential pricing because companies can protect their market dominance through ensuring that consumers buy products or services sold by companies they have partnerships with. *See Consumer Protection Comments, supra* note 45.

⁵⁰ ““One of the issues is the ability to hire technologists,” said Rich, who is now the vice president of consumer policy and mobilization at Consumer Reports. “The FTC simply can’t pay what many technologists make in not-even-the-top echelons of companies.”” Tony Romm, *The Agency in Charge of Policing Facebook and Google is 103 Years Old. Can it Modernize?*, WASH. POST (May 4, 2018), <https://www.washingtonpost.com/news/the-switch/wp/2018/05/04/can-facebook-and-googles-new-federal-watchdog-s-regulate-tech/>; “But we have more cases to bring every day, those cases have become more complex both legally and technologically, and they involve defendants with deep pockets and armies of attorneys. Our budget has not kept pace with these developments...It is critical that the FTC have sufficient resources to support its work, particularly as demands for enforcement in so many complex areas continue to grow.” *Statement of Commissioner Rebecca Kelly*

significantly smaller⁵¹ than it was in the 1980s, while the economy itself has grown three times in size.⁵² That said, it's important to note that more staff — and more technical staff — is not a panacea. Even with a ten- or hundred-fold increase in technologists, the FTC's capacity will invariably be dwarfed by even one medium-sized Silicon Valley company. Such an imbalance cannot be an excuse for failure to take on as daunting a subject matter as algorithmic processing and artificial intelligence. While we strongly believe in the positive possibilities that AI may offer to consumers, so too are the risks that AI may simply be used to trick, manipulate, or coerce users. "Regulatory humility" cannot simply mean regulatory timidity and an abdication of responsibility.

Thank you for the opportunity to comment following the November 13-14, 2018 hearing on algorithms, artificial intelligence, and predictive analytics. If you have any questions, please feel free to contact us at 202.462.6262.

Respectfully submitted,

Justin Brookman
Director,
Consumer Privacy & Technology Policy

Katie McInnis
Policy Counsel

Consumer Reports
1101 17th Street, NW
Suite 500
Washington, DC 20036

Slaughter to the Committee on Energy and Commerce, FED. TRADE COMM'N (July 18, 2018), https://www.ftc.gov/system/files/documents/public_statements/1394982/slaughter_-_prepared_statement_before_use_energy_and_commerce_committee_7-18-18.pdf; "Whatever the means that they choose to adopt, it's time for Congress to take action and provide the FTC with sufficient resources to properly utilize its current enforcement tools." Dylan Gilbert, *The FTC Must Be Empowered to Protect our Privacy*, PUBLIC KNOWLEDGE (June 18, 2018), <https://www.publicknowledge.org/news-blog/blogs/the-ftc-must-be-empowered-to-protect-our-privacy>.

⁵¹ "Our budget has not kept pace with these developments; to wit, we had more FTE in the Reagan administration than we do today." *Statement of Commissioner Rebecca Kelly Slaughter to the Committee on Energy and Commerce*, FED. TRADE COMM'N (July 18, 2018), https://www.ftc.gov/system/files/documents/public_statements/1394982/slaughter_-_prepared_statement_before_use_energy_and_commerce_committee_7-18-18.pdf.

⁵² See Justin Brookman, *What the FTC Really Needs to Deal with Facebook*, IAPP (Nov. 20, 2018), <https://iapp.org/news/a/what-the-ftc-really-needs-to-deal-with-facebook/>.