

Competition and Consumer Protection in the
21st Century Hearings, Project Number P81201
Comment of Dennis Hirsch



Kentucky Law Journal

Volume 103 | Issue 3

Article 3

2015

That's Unfair! Or is it? Big Data, Discrimination and the FTC's Unfairness Authority

Dennis D. Hirsch

Capital University Law School

Follow this and additional works at: <https://uknowledge.uky.edu/klj>

 Part of the [Communications Law Commons](#), and the [Privacy Law Commons](#)
Click here to let us know how access to this document benefits you.

Recommended Citation

Hirsch, Dennis D. (2015) "That's Unfair! Or is it? Big Data, Discrimination and the FTC's Unfairness Authority," *Kentucky Law Journal*: Vol. 103 : Iss. 3 , Article 3.

Available at: <https://uknowledge.uky.edu/klj/vol103/iss3/3>

This Article is brought to you for free and open access by the Law Journals at UKnowledge. It has been accepted for inclusion in Kentucky Law Journal by an authorized editor of UKnowledge. For more information, please contact

That's Unfair! Or is it? Big Data, Discrimination and the FTC's Unfairness Authority

Dennis D. Hirsch¹

INTRODUCTION

Big data is transforming the U.S. economy, spawning new companies and industries at the same time as it generates fresh solutions in the fields of health, education, business, the environment, and many other critical areas.² In but one of many examples, data analysts working with health professionals are using big data to identify those likely to suffer from diabetes and provide these individuals with preventative care.³ “Lest there be any doubt: big data saves lives.”⁴

The picture, however, is not all so rosy. In the absence of legal limits, a company could take the very same ability to identify those who will likely suffer from diabetes and use it to limit these individuals' access to jobs, loans, insurance or housing. Stranger things are already happening. For example, a credit card provider has employed a “behavioral” scoring model to reduce the credit it makes available to those who use their cards to pay for marriage counseling, psychotherapy, billiards, automobile tire retreading, or a number of other disfavored items.⁵ Companies often treat their predictive models as heavily guarded secrets and many such practices are not yet known.⁶ Still, it is clear that a growing number of businesses are using big data to make important eligibility determinations.⁷ Big data

¹ Geraldine W. Howell Professor of Law, Capital University Law School. The author would like to thank Brian Kocak for his superb research assistance and the members of the Kentucky Law Journal for their excellent work in conceiving of, and organizing, the Symposium of which this article is a part.

² See generally VICTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, *BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK* 1–12, 98–122 (2013) (describing the beneficial ways in which big data and data analytics will transform society); Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 243–251 (2013) [hereinafter *Big Data for All*].

³ See, e.g., Press Release, Independence Blue Cross, NYU, NYU Langone Medical Center Collaborate to Detect Early Diabetes, N.Y. Univ. (Apr. 29, 2013) [hereinafter NYU Press Release], available at <http://www.nyu.edu/about/news-publications/news/2013/04/29/independence-blue-cross-nyu-nyu-langone-medical-center-collaborate-to-detect-early-diabetes.html> (describing such a project whereby “machine-learning algorithms [are developed] to spot cases of undiagnosed diabetes and to predict pre-diabetes”).

⁴ MAYER-SCHÖNBERGER & CUKIER, *supra* note 2, at 61.

⁵ Complaint for Permanent Injunction and Other Equitable Relief at 35, *FTC v. CompuCredit Corp.*, No. 1:08-CV-1976-BBM ¶ 75 (N.D. Ga. June 10, 2008), available at <http://www.ftc.gov/sites/default/files/documents/cases/2008/06/080610compucreditcmptsigned.pdf>.

⁶ Pam Dixon & Robert Gellman, *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future* 6 (2014).

⁷ *Id.*, *passim*.

predictions increasingly determine “people’s life opportunities – to borrow money, work, travel, obtain housing, get into college, and far more.”⁸

Such practices can threaten both privacy and equal opportunity.⁹ They injure privacy when, without notice to or the consent of the individuals concerned, they infer and potentially reveal sensitive information such as pregnancy status,¹⁰ sexual orientation,¹¹ political and religious views, or drug use.¹² They can result in unfair discrimination when the disfavored attributes further correlate to a particular race, religion, gender or other protected class so that the model ends up denying important life opportunities to people in these vulnerable groups.¹³

The privacy and discriminatory harms just described are relatively clear. Others, of equal importance, are less so. For example, assume that predictive analytics shows certain people to be more likely to contract adult onset diabetes, and that a lender denies loans to these individuals. Such a practice could be seen as harmful. It infers sensitive information without notice or consent. It may also deny important life opportunities to people who act to keep themselves healthy and so never actually suffer from the disease, thereby frustrating core notions of fairness and free will. Alternatively, the practice could be seen as be socially beneficial if it makes the business more efficient and reduces the overall cost of credit. So, which is it: harmful, or beneficial? The answer is not entirely clear.¹⁴ To ascertain it, one would have to engage in a complicated balancing of benefits and risks. Many companies today are struggling with just such judgment calls.

It is vital that they make them intelligently. This is so first and foremost for the well-being of the individuals concerned. But it is also critical for the big data economy itself. Significant voices are starting to criticize big data for its perceived privacy and discriminatory impacts.¹⁵ Left unaddressed, these concerns could generate a backlash against data analytics that would shackle this emerging sector

⁸ Danielle Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 19 (2014).

⁹ EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 48 (2014), available at http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (“While many applications of big data are unequivocally beneficial, some of its uses impact privacy and other core values of fairness, equity and autonomy.”).

¹⁰ See generally Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.

¹¹ Michal Kosinska, David Stillwell, and Thore Graepel, *Private traits and attributes are predictable from digital records of human behavior*, Proceedings of the National Academy of Sciences, available at <http://www.pnas.org/content/110/15/5802.full.pdf>.

¹² *Id.*

¹³ See generally Solon Barocas & Andrew D. Selbst, *Big Data’s Disparate Impact* 31–43 (Calif. L. Rev., Vol. 104, 2016), <http://ssrn.com/abstract=2477899> (providing examples of such disparate impacts).

¹⁴ See generally Tal Zarsky, *Understanding Discrimination in the Scored Society*, 89 WASH. L. REV. 1375 (2014) (discussing the conceptual difficulties inherent in analyzing big data discrimination).

¹⁵ Brian Fung, *Why Civil Rights Groups are Warning Against Big Data*, WASH. POST (Feb. 27, 2014), <http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/27/why-civil-rights-groups-are-warning-against-big-data/> (explaining that leading civil liberties and civil rights groups are beginning to question big data’s privacy and discriminatory impacts).

for decades to come.¹⁶ In order to prevent this, and so to achieve big data's full potential, society needs way to balance big data's benefits against its potential harms and so to distinguish predictive practices that are in bounds, from those that are not.

Policymakers have largely failed to provide an effective model for making these determinations. The much-heralded 2014 White House report on big data is a case in point. It highlights potential privacy and discriminatory impacts and identifies the "hard question[] we must reckon with: how to balance the socially beneficial uses of big data with the harms to privacy and other values" that it can cause.¹⁷ However, it offers neither an answer to this question, nor even a clear pathway for arriving at one. Companies, government agencies and others that employ big data need a way to distinguish the appropriate uses from the inappropriate ones. Yet they lack access to a broadly-accepted set of guidelines for doing so.¹⁸ This leaves a huge unmet need in the law and policy of data analytics. The field is growing by leaps and bounds. Yet the critical framework needed to define and promote responsible big data practice is missing.

This Article offers a way to fill this gap. Building on prescient work in this area,¹⁹ it argues that the Federal Trade Commission's "unfairness authority" provides a useful, legally-grounded framework for determining whether or not particular big data uses are appropriate or inappropriate, fair or unfair. As will be further explained below, Section 5 of the Federal Trade Commission Act authorizes the FTC to identify, and declare unlawful, "unfair" business acts and practices.²⁰ Two aspects of this authority make it well-suited to addressing big data. First, in determining whether a given act is or is not "unfair," the FTC Act requires the Commission to weigh its costs and its benefits.²¹ The FTC's unfairness authority could, accordingly, provide a vehicle for comparing a given big data use's benefits and harms and so for determining whether it is "fair."

¹⁶ Cf. Julie Brill, Comm'r, Fed. Trade Comm'n, *Big Data and Consumer Trust: Progress and Continuing Challenges* (Oct. 15, 2014) ("[B]ig data will not realize its full potential unless companies, researchers and policymakers work to build consumer trust in the big data enterprise."), available at http://www.ftc.gov/system/files/documents/public_statements/592771/141015brillidppc.pdf.

¹⁷ EXEC. OFFICE OF THE PRESIDENT, *supra* note 9, at 56; see also *Big Data for All*, *supra* note 2, at 244 ("Concluding that a project raises privacy risks is not sufficient to discredit it. Privacy risks must be weighed against non-privacy rewards.").

¹⁸ Two business-oriented think tanks have begun to make strides in this direction. See generally JULES POLONETSKY, OMER TENE & JOSEPH JEROME, *BENEFIT-RISK ANALYSIS FOR BIG DATA PROJECTS* (2014), available at http://www.futureofprivacy.org/wp-content/uploads/FPF_DataBenefitAnalysis_FINAL.pdf (Future of Privacy Forum paper discussing benefit-risk analysis for big data); Center for Information Policy Leadership, *Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance* (Feb. 2013) (same), available at http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Big_Data_and_Analytics_February_2013.pdf. This is testimony to the importance that sophisticated companies put on mapping this terrain.

¹⁹ See Citron & Pasquale, *supra* note 8 at 22 (discussing the use of the FTC's unfairness authority in reference to data analytics); see generally Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S, J. L. & POL'Y INFO. SOC'Y. 425 (2011) (same).

²⁰ Federal Trade Commission Act, 15 U.S.C. § 45(a) (2012).

²¹ *Id.* § 45(n).

The Act also has another advantageous feature. It not only authorizes the FTC to engage in cost-benefit balancing; it also provides it with a framework for doing so. Concerned that the Commissioners would rely too heavily on their own, subjective views on which business activities were or were not fair, Congress instructed the Commission to ground its decisions in “established public policies.”²² This is helpful. In assessing the fairness of big data, the FTC need not—indeed it cannot—immerse itself in intractable, philosophical questions of what constitutes a privacy injury, or what separates beneficial from harmful discrimination. Instead, Congress has instructed it to look to existing laws and policies. Relying on such “established public policies,” the FTC should be able to construct a framework – grounded in law – that will allow it to distinguish beneficial from harmful big data predictions. What are privacy injuries and harmful discrimination? They are what Congress and other policy-making bodies have determined them to be. The FTC feasibly can apply such a criterion. Even before it does so, companies and other big data users can employ it to build a framework for acceptable big data use, reduce their risk and make the big data economy more sustainable.²³

This Article begins by describing big data, the tremendous benefits that it provides, and the potential threats to privacy and equality that it poses. It then provides an account of the FTC’s unfairness authority. It explains how the Commission might use this authority to distinguish big data practices that are appropriate and fair, from those that are not. This raises a significant legal question. Were the FTC to apply its unfairness authority to big data, would it be acting within the scope of its statutory jurisdiction? Is the FTC Act sufficiently broad to encompass such a task? To answer this, the Article turns to the latest word on the FTC’s unfairness authority and the scope of the FTC Act: the 2014 case of *FTC v. Wyndham Worldwide Corp.*,²⁴ currently on appeal to Third Circuit Court of Appeals.²⁵ In an original reading of this much-discussed case, it shows that the *Wyndham* decision both supports FTC’s authority to regulate big data practices and provides further guidance on how the Commission should go about doing so. It concludes that the FTC may well have legal authority to address big data’s negative impacts, and so to unlock its many benefits.

WHAT IS BIG DATA?

Some define big data in terms of its *volume*—the massive data sets that it employs.²⁶ Others add two additional key attributes—big data’s ability to blend and

²² *Id.*

²³ *Cf.* WORLD ECON. FORUM, UNLOCKING THE VALUE OF PERSONAL DATA: FROM COLLECTION TO USAGE (2013) (arguing that a legal framework is needed to reduce big data’s threats and so to unlock its many benefits), available at http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf.

²⁴ 10 F. Supp. 3d 602, 607 (D.N.J. 2014).

²⁵ See generally *FTC v. Wyndham Worldwide Corp.*, No. 14-8091 (3d Cir. filed July 15, 2014) (granting Wyndham Worldwide’s petition for leave to appeal).

²⁶ See, e.g., WORLD ECON. FORUM, *supra* note 23, at 3 n.1 (defining big data as “a collection of

analyze a *variety* of different types of data, and the tremendous *velocity* with which it carries out these operations.²⁷ They put these three elements together and explain big data in terms of “the 3 Vs: Volume, Variety, and Velocity.”²⁸ The three Vs are necessary, but not sufficient, to describe big data. Big data also possesses another attribute that is central to the benefits it creates and the threats that it poses. It uses correlations to generate accurate and actionable predictions.²⁹

A familiar example illustrates the workings and value of this predictive capacity. Amazon.com knows the purchasing history of each of its tens of millions of customers. This allows it to calculate the likelihood, for any two items that it sells, that a customer who purchased one of these items also purchased the other. In most instances, that probability is small. But for some product combinations it is very large. Amazon.com takes these strong correlations and uses them to predict the preferences of its current customers. Where such a customer has purchased or even spent time looking at one of the correlated items, the company predicts that he or she may also be interested in the other. Thus, if one goes on Amazon.com and searches for Harry Potter Paperback Box Set the site will inform the visitor that those who bought this product also purchased the Percy Jackson and the Olympians 5-book paperback boxed set, and the Hunger Games Trilogy boxed set.³⁰ Amazon.com’s correlation-based predictions of consumer preferences have turned out to be highly accurate and valuable. Its recommendation system is responsible for roughly a third of its current sales.³¹ As this example illustrates, “[p]redictions based on correlations lie at the heart of big data.”³²

BIG DATA'S BENEFITS, AND THREATS

The benefits of big data are, in large part, the benefits that flow from this capacity to predict the future. Businesses can make use of this ability. Amazon.com employs it to market its products. Other companies employ big data to predict which new songs are most likely to become popular and purchase the rights to

data sets so large and complex that they become difficult to process using available database management tools or traditional data-processing applications”).

²⁷ Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INT’L DATA PRIVACY L. 74, 82–83 (2013); *IT Glossary: Big Data*, GARTNER, <http://www.gartner.com/it-glossary/big-data> (last visited Jan. 21, 2015).

²⁸ EXEC. OFFICE OF THE PRESIDENT, *supra* note 5, at 4 (internal quotation marks omitted) (defining big data in terms of the three Vs); U.K. INFO. COMM’R OFFICE, BIG DATA AND DATA PROTECTION 6–8 (2014) [hereinafter ICO Report], available at <https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf> (discussing those who use the three Vs to define big data).

²⁹ MAYER-SCHÖNBERGER & CUKIER, *supra* note 2, at 11 (“At its core, big data is about predictions.”); see also ICO Report, *supra* note 28, at 3 (“[Big data] is characterized by volume, variety and velocity of data, and by the use of algorithms, using ‘all’ the data and repurposing data.” (emphasis added)).

³⁰ Search performed by author on Amazon.com (December 4, 2014).

³¹ MAYER-SCHÖNBERGER & CUKIER, *supra* note 2, at 52.

³² See *id.* at 55.

them,³³ or to assess how all Twitter messages (“tweets”) within a certain time period correlate with stock market performance, and so predict how the market is likely to move in the future.³⁴ These are but a few of the many, many business applications for big data.

Big data’s benefits go well beyond the commercial realm. Data analysts use correlations to predict who is likely to get diabetes or other diseases so that they can counsel them on how to avoid these illnesses.³⁵ They use big data to discern which medical treatments are likely to work for which types of people, and so to provide better medical care.³⁶ They employ it to anticipate when a bridge or engine is likely to give out and preemptively repair it before a problem occurs.³⁷ They use it to tell which students are likely to struggle in school and so provide them with the appropriate educational resources.³⁸ In these ways and others big data can enhance health, education, safety and other important social goals.

Big data’s power to predict also has a dark side. It can be employed in ways that harm privacy and equal opportunity. Target’s controversial use of big data helps to illustrate this. Apparently, the best time to get customers to commit to a new retail chain is at the moment of a major life change, such as the birth of a child.³⁹ Target and other retailers accordingly review birth listings, identify those who have recently had a child and mail advertisements and coupons to them.⁴⁰ Several years ago, Target decided to try and get to the new mothers first. It wanted to market baby goods to them when they were *pregnant*. The question was how to determine whether a particular woman was pregnant. Big data provided the answer.⁴¹

Target already possessed a massive database of customer purchases.⁴² By comparing this data with public birth listings and in-store baby shower registries, the company was able to identify about two dozen items that pregnant customers commonly purchased in the months before they gave birth—things like unscented body lotion, calcium supplements, and hand sanitizers.⁴³ It then took this profile and applied it to its database of current customers.⁴⁴ Where a woman had recently purchased many items on the list, Target assigned her a high “pregnancy prediction score”⁴⁵ and sent her baby-related advertisements and coupons.⁴⁶

Some months after the company implemented the strategy a man entered a

³³ See *id.* at 58.

³⁴ *Id.* at 92–93.

³⁵ See *Big Data for All*, *supra* note 2, at 245–47 (providing other examples where statistical data was used to predict patterns in large datasets); NYU Press Release, *supra* note 3.

³⁶ MAYER-SCHÖNBERGER & CUKIER, *supra* note 2, at 60.

³⁷ See *id.* at 58–59.

³⁸ See *id.* at 195.

³⁹ See generally Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.

⁴⁰ *Id.*

⁴¹ See generally *id.*

⁴² *Id.*

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ *Id.*

⁴⁶ See *id.*

Target store and complained that the company was sending his fifteen-year old daughter baby-related coupons.⁴⁷ "Are you trying to encourage her to get pregnant?" he demanded.⁴⁸ The manager apologized profusely and the man left.⁴⁹ Shortly thereafter, the manager called to apologize again and found that the formerly indignant father was now embarrassed and apologetic.⁵⁰ He had had a conversation with his daughter. It turned out that she was pregnant after all.⁵¹ Target had known before he had.

This example helps to illustrate the two main harms that big data's predictive analytics can create. First, Target's mailing of the pregnancy-related coupons to the young woman's home revealed her pregnancy to her father without her consent. This injured her privacy.⁵² To appreciate the second major harm, it helps to modify slightly the facts. Assume that, having figured out who was likely to be pregnant, Target decided to use the insight, not to market baby items, but to deny job interviews to female applicants with high pregnancy prediction scores. Such a practice would privilege men over women. This would constitute a form of invidious discrimination—discrimination against a protected class.⁵³ Many would agree that such actions were harmful, and probably illegal.⁵⁴ Were a company to utilize a profile that *inadvertently* discriminated against a protected class—say, by using an algorithm that sought to deny loans to those most likely to have a heart attack but inadvertently singled out a particular racial group⁵⁵—this might constitute disparate impact discrimination.⁵⁶ The crux of the issue, however, lies in those cases where the harm is even less clear-cut. Assume that a lender employed big data to identify and deny loans to those most likely to suffer a heart attack, and did so without discriminating against a particular racial group or other protected class. Should society see this as a harmful form of discrimination?

This hypothetical is not far from reality. Several large insurance firms have been testing whether they can use data gleaned from a wide variety of online and offline sources to predict which insurance applicants are likely to suffer from high blood

⁴⁷ *Id.*

⁴⁸ *Id.* (internal quotation marks omitted).

⁴⁹ *Id.*

⁵⁰ *See id.*

⁵¹ *Id.*

⁵² DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 142 (2008) (defining the privacy injury of "disclosure" which "occurs when certain true information about a person is revealed to others").

⁵³ Mark MacCarthy, *supra* note 19 at 456 (2011) (defining invidious discrimination as decisions based on "protected categories").

⁵⁴ *See* Pregnancy Discrimination Act of 1978, Pub. L. No. 95-555, 92 Stat. 2076 (codified as amended at 42 U.S.C. § 2000e(k) (2012)); *see also* Darlena Cunha, *When Bosses Discriminate Against Pregnant Women*, THE ATLANTIC (Sept. 24, 2014, 9:15 AM), <http://www.theatlantic.com/business/archive/2014/09/when-bosses-discriminate-against-pregnant-women/380623>.

⁵⁵ *See* Zarsky, *supra* note 14 at 1389-1404 (discussing implicit discrimination of this type).

⁵⁶ *See* Omer Tene & Jules Polonetsky, *Judged by the Tin Man: Individual Rights in the Age of Big Data*, 11 J. ON TELECOMM. & HIGH TECH. L. 351, 358-59 (2013) [hereinafter *Tin Man*] (discussing situations in which apparently neutral data analytics can mask discrimination against a protected class); Barocas, *supra* note 13, at 31-43.

pressure, depression, or diabetes, and so to identify high-risk applicants.⁵⁷ Two leading experts on big data law and policy explain that, with the rise of this new predictive capability, “the danger to us as individuals shifts from privacy to probability: algorithms will predict the likelihood that one will get a heart attack (and pay more for health insurance), default on a mortgage (and be denied a loan), or commit a crime.”⁵⁸ A 2014 White House report entitled *Big Data: Seizing Opportunities, Preserving Values*, concludes that, while predictive scores “may be generated for marketing purposes, they can also in practice be used similarly to regulated credit scores in ways that influence an individuals’ [sic] opportunities to find housing, forecast their job security, or estimate their health, outside of [existing legal protections].”⁵⁹ Federal Trade Commission Chairwoman Edith Ramirez is concerned that predictive inferences will judge individuals “not because of what they’ve done, or what they will do in the future, but because inferences or correlations drawn by algorithms suggest they may behave in ways that make them poor credit or insurance risks, unsuitable candidates for employment or admission to schools or other institutions, or unlikely to carry out certain functions.”⁶⁰

Denying employment, loans, housing, insurance, or other important opportunities and goods to those deemed to be at greater risk of a heart attack would not constitute invidious discrimination since these individuals would not fit the legal definition of “disabled” and so would not be members of a protected class.⁶¹ But would it be harmful? This is not an easy question to answer. Clearly, withholding jobs, loans, insurance, or housing imposes a significant cost on those denied access to them. Moreover, it seems unjust to deny these vital life opportunities to people who may never experience a heart attack and may even take steps to prevent one. From the perspective of the business, however, this sorting produces benefits. Assuming that they can identify those with a greater chance of a heart attack, and that these individuals really do perform less well as employees, borrowers, tenants, and life insurance customers, a company could justifiably be worried about transacting with them.

So is this potential use of big data—and the many others like it—harmful, or

⁵⁷ Leslie Scism & Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients*, WALL ST. J. (Nov. 19, 2010, 12:01 AM), <http://online.wsj.com/articles/SB10001424052748704648604575604575620750998072986>.

⁵⁸ MAYER-SCHÖNBERGER & CUKIER, *supra* note 2, at 17.

⁵⁹ EXEC. OFFICE OF THE PRESIDENT, *supra* note 9, at 46.

⁶⁰ Edith Ramirez, Chairwoman, Fed. Trade Comm’n, Keynote Address at the Technology Policy Institute Aspen Forum: The Privacy Challenges of Big Data: A View from the Lifeguard’s Chair 7 (Aug. 19, 2013), available at http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-challenges-big-data-view-lifeguard-s-chair/130819bigdataaspen.pdf.

⁶¹ To qualify as “disabled” under the Americans with Disabilities Act, a person’s condition must interfere, or be perceived to interfere, with a major life activity. Americans with Disabilities Act of 1990 (ADA), Pub. L. No. 110-325, § 3, 122 Stat. 3553, 3555 (codified as amended at 42 U.S.C. § 12102(1) (2012)) (defining “disability”). For the purposes of the Act “major life activities include, but are not limited to, caring for oneself, performing manual tasks, seeing, hearing, eating, sleeping, walking, standing, lifting, bending, speaking, breathing, learning, reading, concentrating, thinking, communicating, and working.” 42 U.S.C. § 12102(2) (defining “major life activity”). Those who were at risk of a heart attack, but had not yet experienced one, would not meet this definition.

beneficial? That is one of the key questions that big data poses for law and policy, for business,⁶² and for society more generally. As the big data economy continues to grow, it will arise with greater and greater urgency. As was mentioned above, the 2014 White House report on big data frames the problem well. It identifies the central, "hard question[] we must reckon with: how to balance the socially beneficial uses of big data with the harms to privacy and other values" that it can cause.⁶³ The problem is that neither it, nor any other publicly-endorsed set of policies or principles, offers a way to answer this question.

THE FTC'S UNFAIRNESS JURISDICTION

The Federal Trade Commission's Section 5 "unfairness authority" may provide a solution. Section 5 of the Federal Trade Commission Act authorizes the FTC to identify, and enforce against, "unfair or deceptive acts or practices" that affect commerce.⁶⁴ The Commission has largely focused on its "deceptiveness authority," bringing enforcement actions against companies that promise to protect customer data but then, deceptively, fail to do so. When it comes to big data, the question is not so much whether a company acts in accordance with its promises, but whether its actions are appropriate or inappropriate; fair, or unfair. The FTC's unfairness jurisdiction is a promising place to look for a regulatory answer.

Under the Federal Trade Commission Act, the FTC can declare an act or practice to be unfair if it: (1) "causes or is likely to cause substantial injury to consumers;" (2) the injury "is not reasonably avoidable by consumers themselves;" and (3) the injury is "not outweighed by countervailing benefits to consumers or to competition."⁶⁵ These three criteria map well onto big data's predictive profiling. Together, they provide a regulatory mechanism, grounded in existing law, capable of weighing the costs and benefits of particular big data uses and determining, on balance, whether they are beneficial or harmful.⁶⁶

⁶² The Harvard Business Review Blog recently encouraged all companies to think hard about where "value-added personalization and segmentation end[s] and harmful discrimination begins." Michael Schrage, *Big Data's Dangerous New Era of Discrimination*, HARV. BUS. REV.: CUSTOMERS (Jan. 29, 2014), <https://hbr.org/2014/01/big-datas-dangerous-new-era-of-discrimination>.

⁶³ EXEC. OFFICE OF THE PRESIDENT, *supra* note 9, at 56; see also *Big Data for All*, *supra* note 2, at 244 ("Concluding that a project raises privacy risks is not sufficient to discredit it. Privacy risks must be weighed against non-privacy rewards.").

⁶⁴ Federal Trade Commission Act, 15 U.S.C. § 45(a) (2012).

⁶⁵ *Id.* § 45(n).

⁶⁶ In his perceptive article, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, Mark MarCarthy focuses on privacy and personal information generally, rather than on big data. MarCarthy, *supra* note 19, at 426. However, MarCarthy does discuss data mining and, in a very helpful analysis, identifies the potential for discrimination, the need to balance the harms and benefits of personal data use, and the suitability of the FTC's unfairness authority to this end. See *id.* at 454-56, 468, 474-91. Where MarCarthy's article and this one's analysis part company is in their visions of how the unfairness approach should actually work. MarCarthy divides the uses of personal information into three categories: "public benefit use," "the realm of choice," and "impermissible uses." *Id.* at 474-84. As he sees it, data mining injuries other than invidious discrimination fall into the second category and, as such, should be governed by a regime of "notice and affirmative consent." *Id.* at 496. By contrast, as is

Substantial Injury to Consumers

In order to meet the first criterion, a business practice must create a “substantial injury” to a consumer.⁶⁷ These injuries can consist of monetary, economic, health-related, or other types of tangible harm.⁶⁸ Injuries are “substantial” where they are more than “trivial or speculative.”⁶⁹ Clearly, diminished access to jobs, loans, housing, insurance, or other important goods and life opportunities can impose damage that is neither speculative nor trivial. Big data’s privacy and discriminatory impacts accordingly constitute “substantial injuries” and meet the first element of the Section 5 unfairness test.

Not Reasonably Avoidable

Under the second element, these injuries must “not [be] reasonably avoidable by consumers themselves.”⁷⁰ The idea here is that, where consumers are able to avoid injuries through their market choices, it would be paternalistic for the FTC to step in and protect them.⁷¹ Regulatory action is appropriate only where there is an “obstacle to the free exercise of consumer decisionmaking [sic].”⁷² This element seeks to separate those instances in which consumers can protect themselves, from those in which they cannot.

Big data’s privacy and discriminatory harms would appear to fall squarely into the latter category. Few consumers can become aware of and achieve control over the collection of their personal information. Fewer still can understand how companies use data analytics to infer additional information about them and make decisions that affect them. Consumers cannot protect themselves against big data’s privacy or discriminatory impacts through their market choices. These injuries meet the second Section 5 unfairness element.

explained below, this article would apply the cost-benefit balancing approach to all big data applications that injure privacy or equality and would not rely on a notice and consent mechanism.

⁶⁷ *Id.*

⁶⁸ *Int'l Harvester Co.*, 104 F.T.C. 949, 1055 (1984) (reprinting the F.T.C. Policy Statement on Unfairness); MacCarthy, *supra* note 19, at 484; J. Howard Beales, Former Dir., Fed. Trade Comm'n, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection* (May 30, 2003), available at <http://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection> (discussing how the “FTC’s unfairness authority can and should play [an important role] in fashioning [a] consumer protection policy”). There is dispute as to whether purely emotional or dignitary injuries count for these purposes. Compare *Int'l Harvester*, 104 F.T.C. at 1073 (noting that emotional injuries do not count), and Beales, *supra*, at 5 (noting also that emotional injuries do not count), with MacCarthy, *supra* note 19, at 484 (noting that emotional and dignitary injuries do count if a reasonable person would consider it a genuine harm).

⁶⁹ MacCarthy, *supra* note 19, at 484.

⁷⁰ 15 U.S.C. § 45(n) (2012).

⁷¹ Beales, *supra* note 68.

⁷² *Int'l Harvester*, 104 F.T.C. at 1074; Beales, *supra* note 68.

Outweighed by Countervailing Benefits

The third element asks whether the activity's harms are outweighed by its "countervailing benefits to consumers or to competition."⁷³ Courts, commentators and the FTC itself interpret this criterion to require a cost-benefit analysis.⁷⁴ In assessing it, the FTC generally balances the costs that the activity imposes on consumers against the benefits it creates for consumers and for business.⁷⁵

Consider the example set out above in which lenders identify those who have a higher risk of heart attack and then limit these individuals' access to loans. Such practices harm the individuals who been denied credit. They also undermine fundamental societal commitments to fairness and free will. On the other hand, they benefit both to the lenders and consumers who may, as a result of this practice, enjoy lower interest rates. The third element would require the FTC to weigh the harms against the benefits. That is exactly the kind of balancing analysis that society needs to undertake in order to distinguish useful and appropriate big data analyses, from harmful and inappropriate ones.

How to carry out such a balancing? The FTC Act once again offers useful instruction. It states that, "[i]n determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. However, such public policy considerations may not serve as a primary basis for such determination."⁷⁶ As was mentioned above, Congress added this language in 1994 to constrain FTC discretion. Critics had asserted that the Commission was finding business practices to be unfair based solely on its own, subjective view of whether the actions offended "public policy."⁷⁷ Congress sought to make it clear that the FTC must rely on *established* public policies in making such determinations.⁷⁸ It further clarified that the Commission could not rely on established policies as the "primary basis" for its unfairness decisions, but must carefully apply each of the three congressionally-defined unfairness elements. In this way, Congress limited the FTC's unfairness authority and required that the Commission tether its exercise of this power to established legal and policy precedents.

In the big data area, the most relevant "established public policies" concern privacy and discrimination. Thus, in determining whether or not a given big data

⁷³ 15 U.S.C. § 45(n) (2012).

⁷⁴ *Int'l Harvester*, 104 F.T.C. at 1070, 1073 (stating that FTC will not find a practice to be unfair "unless it is injurious in its net effects"); MacCarthy, *supra* note 19, at 487 (stating that the test is whether "the harm is . . . outweighed by a greater social good"); Beales, *supra* note 68 (stating that the Section 5's unfairness prong creates a net benefit test); David L. Belt, *Should the FTC's Current Criteria for Determining "Unfair Acts or Practices" be Applied to State "Little FTC Acts"?*, THE ANTITRUST SOURCE 1, 11 (Feb. 2010), available at http://www.americanbar.org/content/dam/aba/publishing/antitrust_source/Feb10_Belt2_25f.authcheckdam.pdf.

⁷⁵ Beales, *supra* note 68.

⁷⁶ 15 U.S.C. § 45(n) (2012).

⁷⁷ Belt, *supra* note 74, at 2.

⁷⁸ Beales, *supra* note 68; see Belt, *supra* note 74, at 2-3 (discussing the criteria for determining unfairness).

practice is unfair, the Commission should consider such established laws and policies as:

- Constitutional doctrines of privacy, equal protection and due process;
- Privacy statutes such as the Fair Credit Reporting Act;⁷⁹
- Judicially recognized privacy torts;
- Anti-discrimination laws such as Title VII of the Civil Rights Act of 1964 (prohibiting employment discrimination),⁸⁰ the Fair Housing Act,⁸¹ the Americans with Disabilities Act,⁸² and the Equal Credit Opportunity Act;⁸³
- Rules governing racial profiling;
- Statutes, such as the Genetic Information Non-discrimination Act,⁸⁴ that limit companies' ability to use personal information for insurance, employment and other eligibility decisions.
- State laws limiting employer use of employee social media postings for hiring or promotion decisions; and
- The FTC's own unfair business practices precedents.

This existing set of legal and policy doctrines can provide a scaffolding on which the FTC can hang its unfairness determinations. In so doing, it can make the Commission's findings about particular big data practices less subjective, give the FTC established parameters within which to operate, and provide it with a foundation on which to moor its decision-making.

It can also provide much-needed guidance to industry. Months, and perhaps years, will pass before the FTC regulates big data comprehensively. During this period, companies seeking to act responsibly and protect their good reputations will need a framework for determining which big data uses are appropriate, and which are not. Two think tanks have begun to develop risk-based approaches that companies can employ to structure their big data operations.⁸⁵ The Section 5

⁷⁹ 15 U.S.C. §§ 1681-1681x (2012).

⁸⁰ 42 U.S.C. §§ 2000e to 2000e-17 (2012).

⁸¹ 42 U.S.C. §§ 3601-3619 (2012).

⁸² 42 U.S.C. §§ 12101-12213 (2012).

⁸³ 15 U.S.C. §§ 1691-1691f (2012).

⁸⁴ 42 U.S.C. §§ 2000ff to 2000ff-11 (2012).

⁸⁵ See generally POLONETSKY, TENE & JEROME *supra* note 18; Center for Information Policy Leadership, *Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance* (Feb. 2013), available at http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Big_Data_and

unfairness framework offers another set of benchmarks—one grounded, not just on sound thinking, but also on the established legal precedents set out above. Further research is required to synthesize the relevant “established public policies” and arrange them in a framework that big data companies, and the FTC itself, could use to make these fairness determinations.

THE SIGNIFICANCE OF WYNDHAM V. FTC

This Article has argued that the FTC's Section 5 unfairness authority is well suited to the regulation of big data. This assumes that the Commission actually has the legal authority to use its unfairness jurisdiction in this way. Does it?

The FTC's prior experience with its unfairness authority suggests that the answer to this question is anything but clear. In the 1970's, the FTC aggressively employed its unfairness authority to limit business practices that it believed to be unfair.⁸⁶ Critics accused the Commission of assessing unfairness based on the Commissioners' own, subjective views as to which business practices were desirable and which were not.⁸⁷ This ultimately produced a strong political backlash, with Congress at one point even refusing to provide the Commission with necessary funding and forcing it to shut down for several days.⁸⁸ In 1980, the FTC responded with a Policy Statement on Unfairness that defined and constrained its own unfairness jurisdiction.⁸⁹ In 1994, Congress amended the Federal Trade Commission Act to codify the three unfairness elements described above, and to require that the Commission ground its decisions on established public policies rather than on the Commissioners' own policy views.⁹⁰ In the years that followed, the FTC largely refrained from using its unfairness authority and relied, to a far greater extent, on its less controversial deceptiveness jurisdiction.⁹¹

In the past decade or so the Commission, responding to growing challenges of the digital society, has once again begun to employ its unfairness jurisdiction.⁹² Most recently, the FTC has begun to assert unfairness claims against companies

_Analytics_February_2013.pdf.

⁸⁶ Beales, *supra* note 68; Belt, *supra* note 74, at 2.

⁸⁷ Beales, *supra* note 68; Belt, *supra* note 74, at 2.

⁸⁸ See G.S. Hans, Note, *Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era*, 19 MICH. TELECOMM. & TECH. L. REV. 163, 168 (2012); Beales, *supra* note 68; Belt, *supra* note 74, at 2.

⁸⁹ Letter from Michael Pertschuk, Chairman, F.T.C., to Hon. Wendell H. Ford, Chairman, Consumer Subcomm., U.S. Senate, and Hon. John C. Danforth, Ranking Minority Member, Comm. on Commerce, Science and Transp., U.S. Senate, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980), reprinted in *Int'l Harvester Co.*, 104 F.T.C. 949, 1072-76 (1984); see also Hans, *supra* note 88, at 168-69; Beales, *supra* note 68.

⁹⁰ 15 U.S.C. § 45(n) (2012); see also Beales, *supra* note 68; Belt, *supra* note 74, at 4.

⁹¹ See Beales, *supra* note 68 (explaining that, subsequent to the 1994 Amendments, the FTC “showed extreme reluctance to assert its unfairness authority”).

⁹² See Belt, *supra* note 74, at 6 (describing how, starting in 2001, the FTC began using its unfairness authority in “Internet-related enforcement actions”).

whose inadequate data security practices result in data security breaches.⁹³ Following the Federal Trade Commission Act's three criteria, the FTC has maintained that careless data security practices substantially injure consumers are not reasonably avoidable by consumers, themselves, and are not outweighed by the cost savings or other benefits to the company in question.⁹⁴ Until recently, all of the companies against whom the FTC had brought such actions settled with the Commission.⁹⁵

That changed when the FTC brought an enforcement action against Wyndham Worldwide Corporation, the owner of the Wyndham Hotel chain.⁹⁶ The Commission alleged that, as a result of Wyndham's inadequate data security practices, hackers were able to access customers' personal information including "payment card account numbers, expiration dates, and security codes."⁹⁷ In fact, the Commission asserted that these intruders had been able to penetrate Wyndham's system *three times* using similar techniques and that, after discovering the first two breaches, Wyndham had failed to take appropriate measures to prevent the third.⁹⁸ The FTC alleged that, given the hotel chain's public representations about how it would protect customer information, its behavior was deceptive and unfair.⁹⁹

Wyndham fought back. It filed a Motion to Dismiss asserting, among other things, that the FTC's unfairness authority did not reach corporate data security practices.¹⁰⁰ In its Motion, Wyndham compared the FTC's assertion of authority over corporate data security practices to the FDA's effort to regulate tobacco products.¹⁰¹ Just as the Supreme Court in *FDA v. Brown & Williamson Corp.* rejected the FDA's attempt to exercise jurisdiction over tobacco products, the company argued, the District Court should deny the FTC's asserted jurisdiction over data security practices.¹⁰² Companies, policymakers, reporters, and scholars interested in the scope of the FTC's unfairness authority took note, and the litigation has since received wide attention.

On April 7, 2014, the U.S. District Court for the District of New Jersey denied the Motion to Dismiss, a ruling that is currently on appeal to the Third Circuit Court of Appeals.¹⁰³ The court began with the idea that Congress, in Section 5, granted the FTC "broad discretionary authority" to declare business acts and

⁹³ GINA STEVENS, CONG. RESEARCH SERV., R43723, THE FEDERAL TRADE COMMISSION'S REGULATION OF DATA SECURITY UNDER ITS UNFAIR OR DECEPTIVE ACTS OR PRACTICES (UDAP) AUTHORITY 6-7 (2014) (stating that, since 2002, the FTC has settled 20 cases alleging that a company's failure reasonably to protect consumer data constituted an unfair act or practice).

⁹⁴ *Id.* at 3.

⁹⁵ *Id.* at 6-7.

⁹⁶ See generally *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (affirming the FTC's ability to use its unfairness authority in this way).

⁹⁷ *Id.* at 608.

⁹⁸ *Id.*

⁹⁹ *Id.* at 602.

¹⁰⁰ *Id.* at 607.

¹⁰¹ *Id.* at 611.

¹⁰² *Id.*

¹⁰³ See generally *FTC v. Wyndham Worldwide Corp.*, No. 14-8091 (3d Cir. filed July 15, 2014) (granting Wyndham Worldwide's petition for leave to appeal).

practices to be unfair.¹⁰⁴ The FTC should accordingly be able to enforce against unfair data security practices unless the Supreme Court's *Brown & Williamson* decision requires otherwise.¹⁰⁵

The court found *Brown & Williamson* to be distinguishable.¹⁰⁶ It explained that the Supreme Court had rejected the FDA's asserted jurisdiction over tobacco products because Congress had already settled on a "less extensive regulatory scheme" that conflicted with the FDA's effort,¹⁰⁷ and because the FDA had on multiple occasions disclaimed its own authority to regulate tobacco products.¹⁰⁸ By contrast, the court concluded that the FTC's data security unfairness actions complement, rather than conflict with, existing legislation in this area.¹⁰⁹ The court further found that the FTC had not made the kind of "resolute, unequivocal" disclaimer of authority with respect to data security practices that the FDA had made regarding tobacco products.¹¹⁰ Accordingly, the court held that *Brown & Williamson* did not preclude the FTC's assertion of unfairness authority over unduly lax corporate data security practices.¹¹¹ Given this, the Commission's "broad discretionary authority" allowed it to deem such practices unfair.¹¹²

This holding would support FTC's use of its unfairness authority to address harmful big data activities. As with corporate data security practices, an FTC unfairness action against damaging big data practices would not conflict with any existing legislation.¹¹³ In fact, it would be consistent with, and reinforce, the type of privacy statutes, anti-discrimination laws, and other "established public policies"¹¹⁴ on which the Commission would likely base its unfairness determinations. Turning to the second *Brown & Williamson* factor, it seems clear that the FTC has not "resolute[ly] or unequivocal[ly]" disclaimed its authority to declare certain big data practices to be unfair.¹¹⁵ The Commission has said little about this topic. What it has said is consistent with this exercise of authority.¹¹⁶ In short, the FTC's use of its unfairness authority to regulate big data would resemble its regulation of data security practices far more closely than it would the FDA's attempt to regulate tobacco products that the Supreme Court rejected in *Brown & Williamson*. Assuming that the Third Circuit affirms the District Court's ruling in *Wyndham*,

¹⁰⁴ *Wyndham Worldwide Corp.*, 10 F. Supp. 3d at 616 (quoting *Am. Fin. Serv. Ass'n. v. FTC*, 767 F.2d 957, 967 (D.C. Cir. 1985)).

¹⁰⁵ *Id.* at 610-11.

¹⁰⁶ *See id.* at 611-12.

¹⁰⁷ *Id.* at 610-12.

¹⁰⁸ *Id.* at 613-14.

¹⁰⁹ *Id.* at 613.

¹¹⁰ *Id.* at 614.

¹¹¹ *Id.* at 613-15.

¹¹² *Id.* at 615 (quoting *Am. Fin. Serv. Ass'n. v. FTC*, 767 F.2d 957, 967 (D.C. Cir. 1985)).

¹¹³ *Id.* at 613.

¹¹⁴ 15 U.S.C. § 45(n) (2012).

¹¹⁵ *Wyndham Worldwide Corp.*, 10 F. Supp. 3d at 613-14.

¹¹⁶ *See, e.g.*, Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Opening Remarks: Big Data: A Tool for Inclusion or Exclusion? (September 15, 2014), available at <http://www.ftc.gov/news-events/speeches> (stressing the need to evaluate whether big data practices are "unfair, biased, or even illegal discrimination" and whether or not steps can be taken to "level the playing field").

the FTC may well be able to use its unfairness authority to meet the challenges that big data poses. This could turn out to be the true significance of *Wyndham*.

Wyndham not only supports the FTC's ability to employ its unfairness jurisdiction, but also provides important guidance on *how* the Commission can go about doing so. In its Motion to Dismiss, *Wyndham Hotels* argued that, in the absence of any "rules, regulations, or other guidelines" that formally spell out what kind of data security practices the FTC expects under Section 5, any unfairness-based enforcement action violates constitutional principles of fair notice and Due Process.¹¹⁷ The company maintained that the Commission "cannot rely on enforcement actions to make new rules and concurrently hold a party liable for violating the new rule."¹¹⁸ If the FTC wants to use its unfairness authority in this way, it must first set out the standards by which it will do so.¹¹⁹ The court accordingly had to determine "whether fair notice *requires* the FTC to formally issue rules and regulations before it can file an unfairness claim in federal district court."¹²⁰

The District Court concluded that fair notice did not require this practice.¹²¹ Citing a bedrock principle of administrative law, the court stated that the decision on whether to make policy through rulemaking or adjudication "lies in the informed discretion of the administrative agency."¹²² This principle is especially strong in those situations, like the FTC's application of Section 5 unfairness to corporate data security practices, where the legal doctrine at issue is a "flexible" one and the facts to which the agency must apply it are "rapidly-evolving."¹²³ In circumstances such as these, "the problem may be so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule."¹²⁴ The agency is best able to determine this and to decide whether to proceed through rulemaking or case-by-case adjudication.¹²⁵ The District Court accordingly concluded that, in applying a flexible standard like Section 5 to a rapidly changing field such as data security, the FTC was well within its jurisdiction in deciding to make policy through adjudications.¹²⁶ The court went on to explain that the FTC Act itself, with its three-part unfairness test, provides regulated parties with sufficient notice to comport with Due Process.¹²⁷ Over time, the Commission's rulings on data security will elaborate on this statutory standard and create a "body of experience and informed judgment" to which both courts and regulated entities

¹¹⁷ *Wyndham Worldwide Corp.*, 10 F. Supp. 3d at 616.

¹¹⁸ *Id.*

¹¹⁹ *Id.*

¹²⁰ *Id.* at 617.

¹²¹ *Id.*

¹²² *Id.* at 619 (quoting *PBW Stock Exch., Inc. v. SEC*, 485 F.2d 718, 732 (3d Cir. 1973)).

¹²³ *Id.* at 609–10, 619.

¹²⁴ *Id.* at 617 (quoting *SEC v. Chenery Corp.*, 332 U.S. 194, 203 (1947)) (internal quotation marks omitted).

¹²⁵ *Id.* at 617 (citing *SEC v. Chenery Corp.*, 332 U.S. 194, 202–203 (1947)).

¹²⁶ *Id.* at 620.

¹²⁷ *Id.* at 617–19.

"may properly resort for guidance."¹²⁸

The same should hold true for the FTC's application of Section 5's unfairness prong to big data and data analytics. Like data security, big data is a "rapidly-evolving" area.¹²⁹ Big data practices may well present the Commission with problems that are so "varying in nature as to be impossible of capture within the boundaries of a general rule,"¹³⁰ and the FTC, not the courts, will be in the better position to assess this. Just as the District Court held that the FTC could use adjudications to make policy in the realm of data security, other courts will likely hold that it can do so in the field of big data.

This has both advantages and disadvantages. On the negative side, while case-by-case adjudications may provide sufficient notice to comport with constitutional requirements, they inevitably leave some degree of uncertainty as to what, exactly, the FTC will find to be fair or unfair. Businesses will no doubt wish for clearer guidance by which to structure their actions. On the positive side, a case-by-case, adjudicative approach will allow the FTC to proceed incrementally in an area that it does not yet fully understand and so to avoid making generally applicable and rigid rules that do not comport well with business realities. It will further permit the Commission to tailor its rules to the specific circumstances of particular companies and so to implement the unfairness standard in a way that is more in tune with particular circumstances. These virtues are particularly valuable in a still-emerging area such as big data where no one yet knows how the field will evolve and regulatory flexibility and adaptability is key. Assuming that the Third Circuit upholds *Wyndham*, the FTC should be able to proceed in this area through adjudicative policymaking which, even considering the attendant uncertainties, may be better for all concerned.¹³¹

Over time, FTC unfairness adjudications will produce a set of precedents, grounded in "established public policies,"¹³² that will draw a line between appropriate uses of big data, and inappropriate uses; between fair practices, and unfair ones. The FTC is suited to this task and, assuming the Third Circuit affirms *Wyndham*, appears to have the legal authority to pursue it. In the meantime, big data users should be able to employ the unfairness framework to distinguish—in a legally-grounded way—between appropriate and inappropriate big data practices. This is vital to reducing big data's harmful impacts, and so to unlocking and achieving its extraordinary potential.

¹²⁸ *Id.* at 621 (emphasis in original) (quoting *Gen. Elec. Co. v. Gilbert*, 429 U.S. 125, 141-42 (1976)) (internal quotation marks omitted).

¹²⁹ *Id.* at 620.

¹³⁰ *Id.* at 617 (quoting *SEC v. Chenery Corp.*, 332 U.S. 194, 202-203 (1947)) (internal quotation marks omitted).

¹³¹ In their influential work, Professors Solove and Hartzog have argued that this kind of "common law," precedent-building approach to FTC policymaking may, in fact, be a particularly effective way for the Commission to generate a legal framework. See Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 619-625 (2014).

¹³² 15 U.S.C. § 45(n) (2012).

