Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers

Philipp Hacker[†] **& Bilyana Petkova**[‡]

Abstract

The growing differentiation of services based on Big Data harbors the potential for both greater societal inequality *and* for greater equality. Anti-discrimination law and transparency alone, however, cannot do the job of curbing Big Data's negative externalities while fostering its positive effects.

To rein in Big Data's potential, we adapt regulatory strategies from behavioral economics, contracts and criminal law theory. Four instruments stand out: First, active choice may be mandated between data collecting-services (paid by data) and data-free services (paid by money). Our suggestion provides concrete estimates for the price range of a data-free option, sheds new light on the monetization of data-collecting services, and proposes an "inverse predatory pricing" instrument to limit excessive pricing of the data-free option. Second, we propose using the doctrine of unconscionability to prevent contracts that unreasonably favor data-collecting companies. Third, we suggest democratizing data collection by regular user surveys and data compliance officers partially elected by users. Finally, we trace back new Big Data personalization techniques to the old Hartian precept of treating like cases alike and different cases – differently. If it is true that a speeding ticket over $50 is less of a disutility for a millionaire than for a welfare recipient, the income and wealth-responsive fines powered by Big Data that we suggest offer a glimpse into the future of the mitigation of economic and legal inequality by personalized law. Throughout these different strategies, we show how salience of data collection can be coupled with attempts to prevent discrimination and exploitation of users. Finally, we discuss all four proposals in the context of different test cases: social media, student education software and credit and cell phone markets.

Many more examples could and should be discussed. In the face of increasing unease about the asymmetry of power between Big Data collectors and dispersed users, about differential legal treatment, and about the unprecedented dimensions of economic inequality, this paper proposes a new regulatory framework and research agenda to put the powerful engine of Big Data to the benefit of both the individual and societies adhering to basic notions of equality and non-discrimination.

[†] Postdoctoral Fellow, Humboldt University of Berlin; LL.M. (Yale)

[‡] Postdoctoral Max Weber Fellow, European University Institute and Visiting Fellow, Yale Law School Information Society Project, M.S.L (Yale).

This paper has benefited from comments by Chris Jay Hoofnagle, Markus Düttmann, Greg Kimak, and participants in the conference "Unlocking the Black Box: The Promise and Limits of Algorithmic Accountability in the Professions", held on April 1-2 at the Yale Law School, the 2nd Berlin Center for Consumer Policy Forum, held on April 13 at the Berlin Science Center (WZB), as well as a M-EPLI talk at the Maastricht European Private Law Institute, held on April 26. All errors remain entirely our own.

Table of Contents

I. Big Data and the Law: Major Challenges 5
1. Big Data Exacerbating Inequality 6
2. Big Data Mitigating Inequality 10

II. Regulatory Solutions 11
A. Parceling out Transparency 11
1. The Limits of Transparency-as-Accountability 13
2. The Limits of Transparency-as-Consumer-Disclosure 15
B. Substantial Regulation 16
1. Toward a Real Choice between Payment with Money and Payment with Data: Forcing Data Free Services 17
2. Unconscionability and Ex Post Evaluation 23
3. Democratizing Data Collection and Processing 26
4. Wealth- or Income-Responsive Fines 27

III. Test Cases 31
A. Social Media 31
B. Student Education Software 34
C. Credit Card and Cell Phone Markets 36

IV. Conclusion 37

The promise of Big Data is big indeed: thanks to algorithms, clinical research allows seemingly unrelated symptoms to uncover the adverse effects of medicines; "smart grids" reduce energy consumption; congestion and pollution levels in cities can decline; and tailor-made education can bring about better learning results.[1]

However, the side effects of new Big Data techniques have revealed both consumer protection and discrimination issues that lead us to an ever more unequal society. In addition to problems for consumers, Big Data poses greater risks to vulnerable groups. Since basic life opportunities are based on predictive scoring, people are sorted into the "wheat" and the "chaff" for, *inter alia*, their health, housing, employment and travel opportunities.[2] Opaque or incorrect scoring may result in significantly worsened economic conditions for those negatively affected.[3] Moreover, personalization can disadvantage individuals when it is predicated on negative assumptions embedded in the very structure of the algorithm or biased

[1] Omer Tene and Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63 (2012).

[2] FRANK PASQUALE, THE BLACK BOX SOCIETY. THE SECRET ALGORITHMS THAT CONTROL MONEY INFORMATION 3-11 (2015), Chapter 2; Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 13-16 (2014).

[3] Id. at 13-16; *See* CHRIS J. HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2015), Chapter 10.

towards the preferences of a statistical majority.[4] As the "scored society"[5] unfolds, every inch of the lives of individuals is recorded, measured, quantified and analyzed by an increasing array of data-collecting companies, data brokers and software tools. In the year 2013 alone, Big Data companies that use consumer-level data to market and retain consumers have generated total revenue of roughly $165 billion in the United States.[6] That amount is set to rise in the coming years. Academics have extensively examined the impact of unilateral access to behavioral algorithms in the area of personalized advertising[7], showing how adverse targeting leads to suboptimal contracts.[8] In the words of Ryan Calo, "firms have an incentive to engage in individualized 'market manipulation' whereby each consumer is targeted on the basis of his or her specific set of biases or approach at a time when he or she is most vulnerable."[9]

However, this bleak picture conceals the potential of personalization through Big Data for the law of the future. Smart technologies enable differentiation of market transactions on a hitherto unprecedented scale. Depending on the underlying rationale for differential treatment, Big Data can be used to either entrench illegitimate discrimination or to reduce inequality. As with every new technology, this ambivalence is deeply inscribed into the very code of Big Data. The challenge for the legal regime would be to facilitate the positive externalities of Big Data while reining in its potentially discriminatory use.

Algorithmic transparency and due process[10] are suggested as a necessary procedural antidote to some of the Big Data malaise. People not only deserve to be able to access and correct their information but also to know how they are rated and ranked.[11] Importantly, the Snowden revelations have demonstrated how social awareness can bring about reforms in other areas of privacy concern.[12] Transparency regulations moreover carry a "relative political

---

[4] Barocas & Andrew Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. (forthcoming, 2016).

[5] Moreover, in the wake of the Big Data economy, research has shown that government use of database screening can create blacklists of individuals and virtually reverse the presumption of innocence. *See* Margaret Hu, *Big Data Backsliding*, 67 FLA. L. REV. 1735 (2015). Equally troubling, search engines are said to be able to influence election outcomes, Robert Epstein & Robert E. Robertson, *The Search Engine Manipulation effect (SEME) and its possible impact on the outcomes of elections*, American Institute for Behavioral Research and Technology, (2015), available at http://www.pnas.org/content/112/33/E4512.full.pdf.

[6] Katy Bachman, *Big Data Added $156 Billion in Revenue to Economy Last Year*, AdWeek (October 14, 2013), *available at* http://www.adweek.com/news/technology/big-data-added-156-billion-revenue-economy-last-year-153107.

[7] Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014).

[8] Emir Kamenica, Sendhil Mullainathan & Richard Thaler, *Helping Consumers Know Themselves*, 101 AM. ECON. REV. PAPERS & PROCEEDINGS 417, 418 (2011) (reporting on adverse targeting, i.e., the conscious offer of sub-optimal contracts by companies to clients on the basis of the superior information of companies about the future use and spending patterns of their clients).

[9] *Supra* note 8.

[10] Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 BOSTON COLL. L. REV. 93 (2014).

[11] Citron & Pasquale, *supra* note 2; PASQUALE, *supra* note 2.

[12] The Snowden revelations triggered a significant public debate and legislative overhaul of surveillance measures that eventually led to the replacement of the Patriot Act with the USA Freedom Act of 2015. *See* Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015. P. L. 114-23, §1(a).

ease"[13] and smart disclosure policies such as "visceral notice"[14] are proposed to help consumers make better-informed choices about services powered by data. But can transparency work on its own to combat troublesome discriminatory uses of Big Data or do we need to think of other methods of regulation?

While much ink has been spilled on remedying behavioral market failures that arise from personalized advertising,[15] adverse targeting[16] or more generally, the interplay of competition and cognitive biases,[17] legal scholarship has only recently started to discuss regulatory solutions that address harms generated by Big Data. The current article adds to this debate by making two propositions. First, unlike in other areas where federal law and the courts are struggling to translate privacy losses into privacy harms,[18] the unfair techniques with which data might be extracted for analytics can result in tangible economic harms that might substantially disadvantage some individuals.[19] We show how Big Data can multiply discrimination in new and subtle ways. Second, we demonstrate how individualization through Big Data can actually be deployed to fight discrimination more effectively. Ultimately, we suggest regulatory strategies that couple transparency with some substantive protections to eliminate the danger of multiplying inequality through Big Data and instead enhance the prospect of improving equality.

In Part I we outline the main challenges for the law posed by Big Data: first, we argue that through "smart discrimination" and "dual valence correlations", Big Data is able to take societal inequalities to the next level. Second, we unearth Big Data's less-explored potential for remedying inequalities. In Part II, we outline the limits of some of the traditional approaches to Big Data in what we call "transparency as accountability" and "transparency as disclosure". Thus, we develop a framework for reining in the big promise of Big Data through opening a new research agenda that combines transparency with substantial regulation in the area of Big Data. First, to prevent discrimination, we propose concrete strategies for offering data-free services next to unconscionability and the ex post evaluation of contracts. We furthermore look into democratizing data collection as a regulatory tool. Finally, the paper is the first to suggest income or wealth-responsive fines as a way of remedying inequalities through the use of Big Data. Part III tests our premises in three case studies: social media, student education software and credit and cell phone markets. Part IV presents the tentative conclusions.

---

[13] Lauren Henry Scholz, *Privacy Petitions and Institutional Legitimacy*, CARDOZO L. REV (2016), forthcoming.

[14] Ryan Calo, Against Notice Skepticism in Privacy (and Elsewhere), 87 NOTRE DAME L. REV. 1027 (2012).

[15] *See, e.g.*, Frederik Zuiderveen Borgesius, Improving Privacy Protection in the Area of Behavioural Targeting (2015).

[16] Kemanica, Mullainathan & Thaler, *supra* note 8.

[17] *See, e.g.*, Oren Bar-Gill, Seduction by Contract (2012); Cass Sunstein, Choosing not to Choose (2015).

[18] Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND . L.J. 1131, 1132 (2011).

[19] For a categorization of harms provoked by algorithmic decision-making, *see* Pauline T. Kim, *Data-Driven Discrimination at Work*, WM. & MARY L. REV., forthcoming (2017).

I. Big Data and the Law: Major Challenges

Data analytics lead to the greater personalization of services. Before the advent of Big Data, consumers would for the most part see the same advertisements and receive the same offers. However, Big Data has changed the rules of the game. Individuals are treated differently now, based on their metadata such as browsing history, shopping attitudes or the articles they read in electronic newspapers. At a first level, this creates a problem of awareness, salience and consent. As has been noted by numerous scholars, recent surveys suggest an unease of consumers and users with data collection and data mining. A survey conducted in 2015 by the Pew Research Center shows that only 7% of US adults were somewhat or very confident that their record would remain private and secure with online advertisers.[20] 50% of US adults would like to prevent online advertisers from saving records of their activity for any length of time;[21] and more than 90 % of US adults would like to be in control about the information others can get from them.[22] In the 2014 Pew Research Center survey, more than nine out of ten US adults noted that consumers have lost control over the online collection and use of data by companies.[23] Nonetheless, the vast majority of citizens continue to use data-collecting services such as Google or Facebook without sufficiently protecting their privacy by means of proxy servers, encryption, TOR, or other technical standards.[24] This points to a flagrant attitude-action gap that regulation, including the tools we shall propose, can help close. Consumers often do not have the necessary technological knowledge to defend a pro-privacy stance, even if they wanted to. Further, lock-in or network effects explain why many users of social networks remain faithful to the services they receive, even if their privacy gets compromised.[25] The market does not seem to offer effective mechanisms to narrow the attitude-action gap on its own and the consequences can be dire, especially for vulnerable groups.

Importantly, however, we argue that at a second level, beyond privacy concerns and consent, the growing differentiation of services based on personal data harbors the potential for both greater societal inequality *and* for greater equality, i.e., that Big Data is instrumental for both more and less discrimination.[26] The reason for the Janus-faced character of personalization can be traced back to Hart's precept of treating like cases alike and different cases – differently.[27] This basic tenet is reflected to some extent in the US constitutional

---

[20] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Research Center (May 20, 2015), available at http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/, at 7.

[21] Madden & Rainie, *supra* note 20, at 9.

[22] Madden & Rainie, *supra* note 20, at 5.

[23] Pew Research Center, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Report (Nov. 12, 2014), available at http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/, at 3.

[24] Madden & Rainie, *supra* note 20, at 8-9.

[25] In order to fight lock-in effects, in 2012 the European Commission proposed a far-reaching data portability right in its data privacy legislative reform package. The currently adopted EU-wide general data protection regulation introduces a mellowed down version of the right. *See* Art. 20 of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. 2016, L 119/1.

[26] This applies both to intentional discrimination and remedial discrimination.

[27] H.L.A. Hart, *Positivism and the Separation of Law and Morals*, 71 HARV. L. REV. 593, 599 (1958).

tradition of antisubordination that "impugned facially neutral practices with a racially disparate impact, while legitimating affirmative action"[28] and it has also been spelled out by the European Court of Justice as "…[d]iscrimination consists solely in application of different rules to comparable situations or in the application of the same rule to differing situations".[29] Treating different individuals differently is not *per se* tantamount to discrimination or fostering inequality. Rather, the core question becomes whether the respective situations are comparable, which in turn depends on whether good reasons can be advanced for distinguishing one individual from another. The ambivalent dimension of Big Data rests upon the fact that differential treatment can be attached to a variety of personal characteristics and deployed to either combat or entrench discriminatory practices.

1. Big Data Exacerbating Inequality

Next to problems generally associated with consumer protection, the use of Big Data creates inequality whenever it facilitates the differentiation between persons based on traits of their personality or patterns of their behavior thought to be discriminatory, such as traits identified within a protected class under Title VII of the Civil Rights Act of 1964.[30] As Danielle Citron and Frank Pasquale,[31] Solon Barocas and Andrew Selbst[32], as well as Tal Zarsky[33] and others[34], have persuasively argued, the use of correlations uncovered by data science gives rise to inequality on an unprecedented scale triggered by what we term here "smart discrimination". Consider the example of racial discrimination: in the old days, this type of discrimination was often rather obvious. The refusal to sell goods to consumers because of the color of their skin, or even the refusal to ship merchandise to ZIP code areas predominantly inhabited by African-American or Latino communities was a clear sign of racial discrimination.[35] This is not to say that more subtle forms of discrimination did not exist before the advent of Big Data.[36] However, one of the striking characteristics of the era of Big Data is the ability to uncover counterintuitive correlations. Therefore, it is now possible to differentiate seemingly neutral characteristics that, while unnoticed by the general public, correlate with discriminatory traits. Examples include the distance from home to work (which can correlate with racial background),[37] criminal records (which can correlate with racial

---

[28] Jack M. Balkin & Reva B. Siegel, *The American Civil Rights Tradition-- Anticlassification or Antisubordination?*, 2 ISSUES IN LEGAL SCHOLARSHIP 1, 12 (2003).

[29] E.C.J. 1984, 283/83, Racke v Hauptzollamt Mainz, E.C.R. 1984, 3791, paragraph 7.

[30] 42 U.S.C. §§ 2000e-2000e-17.

[31] Citron & Pasquale, *supra* note 2.

[32] *Supra* note 4.

[33] Tal Z. Zarsky, *Understanding Discrimination in the Scored Society*, 89 WASH. L. REV. 1375 (2014).

[34] *See, e.g.*, Toon Calders and Indrė Žliobaitė, *Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures*, *in* DISCRIMINATION AND PRIVACY IN THE INFORMATION SOCIETY 43 (Bart Custers, Toon Calders, Bart Schermer, and Tal Zarsky eds., 2013).

[35] *Cf.* Toon Calders & Sicco Verwer, *Three Naïve Bayes Approaches for Discrimination-Free Classification*, 21 DATA MINING & KNOWLEDGE DISCOVERY 277, 278 (2010); Zarsky, *supra* note 25, at 1394-95.

[36] See, e.g., Devah Pager & Hana Shepherd, *The Sociology of Discrimination: Racial Discrimination in Employment, Housing, Credit, and Consumer Markets*, 34 ANNU. REV. SOCIOL. 181 (2008).

[37] Don Peck, *They're Watching You at Work*, THE ATLANTIC (Nov. 20, 2013), available at http://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-youat-work/354681/ (citing

background),[38] or individual working days versus holidays (which indicate religious beliefs)[39]. If these correlations become implemented into the search algorithms of platforms offering goods and services, Big Data would allow for subliminal forms of discrimination to which we turn below.

a) Dual Valence Correlations

Why would the providers of platforms implement such discriminatory strategies in the first place? The answer is fourfold: First, discrimination can be based on institutional arrangements that follow patterns of implicit, rather than intentional, bias.[40] Institutional discrimination has received significant attention in the sociological literature[41] and might be considered a key driver of the persistence of discrimination in the post-civil rights era. This is also highlighted by the so-called 'Podesta Report' on the ambivalent impact of Big Data issued by the Executive Office of the President.[42] Second, the machine learning procedure may perpetuate biases inherent in the data used to train the algorithm, an issue we address in more detail below.[43] Third, it might be the case that the provider either harbors explicit discriminatory feelings or gains utility by discriminating against consumers based on their racial background, sexual orientation etc.[44] Fourth, there is the so-far underappreciated[45] potential for discrimination arising from the interplay of market forces in which the providers themselves are neutral but they respond to the discriminatory preferences of other market actors. As Christine Jolls and Ian Ayres have persuasively argued, such "rational" discrimination can be the product of profit maximization under certain constraints.[46]

While others have dealt with the first example (institutional discrimination),[47] we now turn to some cases that illustrate the other three categories just mentioned. A problem of inequality arises when certain parameters along which offers are personalized have a dual valence, i.e., when they correlate in a statistically significant way both with traits that would

---

the case of "Evolv", an employment consultancy, which leaves this variable out of their models for fear of discrimination).

[38] Kathleen Daly & Michael Tonry, *Gender, Race, and Sentencing*, 22 CRIME & JUSTICE 201 (1997).

[39] Zarsky, *supra* note 25, at 1395.

[40] This is the form of discrimination Barocas and Selbst focus on, see Barocas & Selbst, *supra* note 4, at 3-4.

[41] See, e.g., Pager & Shepherd, supra note 36, at 185, 198; Jomills Henry Braddock II & James M. McPartland, *How Minorities Continue to Be Excluded from Equal Employment Opportunities: Research on Labor Market and Institutional Barriers*, 43 J. SOC. ISSUES 5 (1987).

[42] EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf, at 45-47.

[43] *See infra*, notes 48 et seqq. and accompanying text.

[44] *See, e.g.*, Zarsky, *supra* note 25, at 1385-86.

[45] *But see* Alistair Croll, *Big Data Is Our Generation's Civil Rights Issue, and We Don't Know It*, SOLVE FOR INTERESTING (July 31, 2012), at http://solveforinteresting.com/big-data-is-our-generations-civil-rights-issue-and-we-dont-know-it/; however, discussion in the legal literature of market forces leading to discrimination has been scarce so far, with the partial exception of Barocas & Selbst, *supra* note 4, at 22-23, 44, and a brief mentioning in Zarsky, *supra* note 25, at 1387.

[46] Christine Jolls, *Antidiscrimination and Accommodation*, 115 HARV. L. REV. 642, 685-86 (2003); Ian Ayres, *Fair Driving: Gender and Race Discrimination in Retail Car Negotiations*, 104 HARV. L. REV. 817, 842-44 (1991).

[47] See *supra*, note 40.

constitute a legitimate reason for differentiation and with discriminatory traits.[48] Let us consider the hypothetical case of an online platform that sells used cars. In deciding whether to make an offer to a potential buyer, the platform provider analyzes the payment history of the buyer on the basis of information they collect on their own and through related platforms; furthermore, as far as possible, the provider gathers information on the buyer's credit history. From the data, the platform calculates a combined credit and payment score (CCPS). To potential buyers with a better CCPS, the platform makes cheaper offers for the same types of cars than to buyers with a worse CCPS. The platform provider defends this strategy by noting that buyers with a lower CCPS are more costly since they are more likely to default on their payments. Taken on its own, this would constitute a sufficient economic reason for price discrimination.[49] However, let us further assume that the CCPS also correlates with racial characteristics: African-Americans, for an intricate set of reasons stemming largely from the educational system,[50] tend to have lower CCPSs. Thus, the algorithm provides the car dealer with a tool to discriminate against African-American consumers while pretending to follow an economic rationale. This concern is not entirely theoretical: in a much-cited study conducted before the advent of Big Data, Ian Ayres and colleagues were able to show how car dealers' offers depend heavily on the racial background of the offeree, with African-American consumers getting worse deals than white consumers.[51] If anything, Big Data can exacerbate the trend.

Certainly, economic reasoning linked to the risk of default has been used in the past to veil discrimination. Big Data, however, presents an entirely new stage in the history of discrimination precisely because it allows for so far unnoticed correlations to take center stage. Even seemingly mundane and harmless characteristics of personalization might mask illegitimate discriminatory preferences.[52] This is particularly problematic in the case of dual valence correlations since the "legitimate correlation" may present a sufficient justification to pass the antidiscrimination test under the disparate treatment[53] and the disparate impact

---

[48] *Cf.* Toon Calders & Sicco Verwer, *Three Naïve Bayes Approaches for Discrimination-Free Classification*, 21 DATA MINING & KNOWLEDGE DISCOVERY 277, 279 (2010); Zarsky, *supra* note 25, at 1389; Barocas & Selbst, *supra* note 24, at 20-22.

[49] Cf. Akiva A. Miller, *What Do We Worry about When We Worry about Price Discrimination - The Law and Ethics of Using Personal Information for Pricing*, 19 J. TECH. L. & POL'Y 41, 70-74 (2014). ADD REFERENCE FROM PAULINE

[50] *See, e.g.,* Richard Wilkinson & Kate Pickett, The Spirit Level. Why Greater Equality Makes Societies Stronger, Chapter 8 (2011).

[51] Ian Ayres & Peter Siegelman, *Race and Gender Discrimination in Bargaining for a New Car*, 85 AM. ECON. REV. 304 (1995). This narrative is part of a broader problem: as computer scientists have pointed out, it is extremely difficult to construct attributes with predictive quality that are uncorrelated to any discriminatory traits. *See, e.g.,* Calders & Verwer, *supra* note 43 at 278 (noting that "simply removing the sensitive attribute from the training dataset does not solve the problem, due to the so-called "red-lining effect", i.e., indirect discrimination through correlations). Therefore, whichever target variable is chosen for data mining, there will always be a potential for – conscious or unconscious – discrimination.

[52] *Cf.* Barocas & Selbst, *supra* note 4, at 23.

[53] *See* McDonnell Douglas Corp. v. Green, 411 U.S. 792, 802 (1973) (noting that once the plaintiff establishes a *prima facie* case of discrimination, the "burden then must shift to the employer to articulate some legitimate, nondiscriminatory reason for the employee's rejection"); Price Waterhouse v. Hopkins, 490 U.S. 228, 229 (1989) (holding that if a mix of motives led to a decision by an employer, one of the motives being illegitimate, "the defendant may avoid a finding of liability by proving by a preponderance of the evidence that it would have made the same decision even if it had not taken the plaintiff's [discriminating feature] into account").

doctrine[54] of Title VII.[55] The current account of the antidiscrimination doctrine holds that disparate treatment cases concern intentional discrimination based on a protected characteristic such as gender or race, while disparate impact cases target practices that are facially neutral but might have discriminatory effects. However, due to the currently narrow interpretation of "disparate impact" by the Supreme Court, antidiscrimination law alone does not seem equipped to deal with the cases we described above.[56] Therefore, the law has to leave the comfortable path of traditional antidiscrimination law to fight these new types of data-driven discrimination. This is what Part II.B. of the article will deal with.

b) "Smart Discrimination"

Next, consider the example of a platform offering apartments for rent. As is well known, some landlords unfortunately have a penchant for white and well-educated tenants.[57] Let us further suppose that access to the platform is free for potential tenants but costs a service fee to the landlords when they offer their apartments for rent. The provider will have an incentive to implement a discriminatory search algorithm under two conditions: First, she must know of the discriminatory preferences of the landlord, which can be reasonably assumed; second, the discriminatory strategy must not be noticed by the majority of the persons discriminated against. Under these conditions, algorithmic discriminatory strategies act as a screening device to channel the "better"-potential tenants, e.g., the white and well-educated, to the landlords' offers. The landlords' willingness to pay a higher service fee to the provider will depend on the perceived "quality" of the applicants they receive through the platform, thus creating an additional incentive for the provider to channel the kind of tenants landlords would like to see responding to their respective offers. However, the success and popularity of the platform would also depend on having as many users as possible. Therefore, an openly discriminatory strategy would, beyond legal concerns, be also economically inefficient. Thus, the provider will have an incentive to tweak the algorithm in a way that, for non-white users, rearranges the hit list of apartments. If, moreover, service fees are coupled to monthly rent, the more expensive apartments will be more profitable for the provider. Ultimately, maximizing the satisfaction of apartment owners will be of the highest priority for the platform provider. An economically efficient discriminatory search strategy could therefore rearrange the hit list of apartments so that the more expensive ones are first shown to white users. This would hinder access to high-quality housing for the non-white users.

---

[54] *Cf.* 42 U.S.C. § 2000e-2(k)(1)(A)(i) (establishing that a hiring practice with disparate impact is legitimate if it is job-related and a business necessity); *see also* Barocas & Selbst, *supra* note 4, at 41 (noting that "there is good reason to believe that any or all of the data mining models predicated on legitimately job-related traits pass muster under the business necessity defense").

[55] On business justification in the context of Title VII, see Jolls, *supra* note 37, at 665-66; Richard A. Primus, *Equal Protection and Disparate Impact: Round Three*, 117 HARV. L. REV. 493, 518, 522 (2003); for a detailed analysis of discriminatory data mining in the light of Title VII, see Barocas & Selbst, *supra* note 4, at 24-46.

[56] But *see* Pauline T. Kim, *supra* note 19. Kim suggests a revisionist reading of Title VII that advances a prohibition on classification bias in the employment context. We are sympathetic to this reading of the text that optimizes the advantages of workforce analytics while curbing its risks. However, with Kim, we are skeptical too since, as she writes, "existing doctrinal forms often exert gravitational pull on our thinking".

[57] Pager & Shepherd, *supra* note 36, at 182-83; John Yinger, *Measuring Racial Discrimination with Fair Housing Audits: Caught in the Act*, 76 AM. ECON. REV. 881 (1986).

The described effect is particularly relevant to areas of the law that ban discrimination in public offerings of goods or services. Examples include the US Fair Housing Act[58] or Section 1981 and 1982 of the Civil Rights Act[59] and in Europe – the EU Antidiscrimination Directive[60]. However, a similar effect can also raise Title VII employment cases if the employer reckons that their customers or coworkers will have discriminatory preferences and decides to adapt his or her recruitment policy accordingly.[61] We see Big Data opening the realm of hidden or "smart" discrimination, which can go unnoticed by those discriminated against. Algorithmic discriminatory strategies might be used either by persons actively wanting to discriminate against others or by those who seek to maximize their revenue. The use of algorithms creates unfortunate economic incentives for "dual valence" and "smart" discrimination.

2. Big Data Mitigating Inequality

While in new and subtle ways Big Data undoubtedly harbors the potential of taking illegitimate discrimination to the next level, Big Data might also contribute to greater economic equality. For several years now both lawyers and economists have been debating the impact of mounting economic inequality in Western societies and what the potential strategies could be to battle this worrying tendency with renewed vigor.[62] Conspicuously left out of the picture so far is the far-reaching potential for mitigating economic inequality by organizing both markets and the legal system by means of Big Data. Ideally, the very same strategies used to decrease economic inequality simultaneously serve to foster legal equality. In Part II, we shall argue that wealth- and income-responsive fines fulfill this dual condition.[63]

The preceding discussion has demonstrated the opportunity structures that Big Data creates for "dual valence" and "smart discrimination". However, the same strategies can be inversed to differentiate between different market actors in a legitimate way. Imagine the aggressive tendencies of the discriminating car dealer just contemplated when the price charged for a certain good is actually *positively* correlated with the income or wealth of the offeree. Anecdotal evidence suggests that Amazon is in fact already using such price discrimination strategies to demand higher prices from Mac vis-à-vis Windows users, the rationale being that the average consumption budget of a Mac user is higher than that of a Windows user.[64] If the type of operating system used is indeed a fair proxy for one's consumption budget, which in turn depends crucially on income and wealth, then the strategy used by Amazon does incrementally lower economic inequality. A similar effect can be

---

[58] 45 U.S.C. §§ 3601-3619.

[59] *See* Ayres, *supra* note 37, at 821.

[60] Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ 2000 L 180/22, Art. 3(1)(h).

[61] *See* Jolls, *supra* note 37.

[62] THOMAS PIKETTY, CAPITAL IN THE TWENTY-FIRST CENTURY (2014); FRANÇOIS BOURGUIGNON, THE GLOBALIZATION OF INEQUALITY (2015); JOSEPH E. STIGLITZ, THE PRICE OF INEQUALITY. HOW TODAY'S DIVIDED SOCIETY ENDANGERS OUR FUTURE (2012); RICHARD WILKINSON & KATE PICKETT, THE SPIRIT LEVEL. WHY GREATER EQUALITY MAKES SOCIETIES STRONGER (2011); David Grewal, *The Laws of Capitalism*, 128 HARV. L. REV. 626 (2014).

[63] *Infra*, Part II.B.4.

[64] Christoph Kucklick, Die granulare Gesellschaft. Wie das Digitale unsere Wirklichkeit auflöst [The Granular Society. How Digitization Dissolves our Reality] 129-30 (2014).

achieved by geostrategic pricing in which the price of a good is determined by the location of the IP address of the user or by the ZIP code of the shipping address[65]. The law, we suggest, can use similar data-driven strategies to combat economic and legal inequality in unprecedented ways.

II. Regulatory Solutions

This brings us to a discussion of potential regulatory solutions for the challenges just described. Simple bans on data collection would often not work, either because they are overreaching, potentially unconstitutional[66] and politically inopportune, or because the huge advantages of data collection and processing for companies, but also partially for consumers, would immediately create a black market with even less oversight. What may be contemplated, however, are some mild regulatory steps designed to minimize the harms of discriminatory uses of Big Data and enhance equality through data collection and processing.

The first and most frequently promoted regulatory tool puts an emphasis on transparency. We outline the different contexts in which transparency-as-accountability and transparency-as-disclosure to the consumer is evoked. However, the limits of disclosure brought about with new empirical research in behavioral and experimental economics lead us to consider, as a second step, substantial forms of regulation. By decreasing company access to citizen data, they aim not only at making citizens aware of the algorithms that sort them, potentially reducing the attitude-action gap in the privacy domain, but more importantly – at significantly limiting the amount of data available to companies in the first place. If data is the source of discrimination in the digital age, reducing the availability of the data of *some* users will reduce the potential for discrimination. This particularly holds true if vulnerable groups are given the possibility to opt out of data collection. Furthermore, the regulatory tools we contemplate leverage Big Data in novel ways to combat economic and legal inequality. In order to explain the necessity for such proposals, however, we shall first critique the current focus on transparency as an absolute antidote to data-driven evils.

A. Parceling out Transparency

Transparency figures prominently on the agenda of rule makers: be it as a part of the revived[67] parlance of 'good governance' of the 2000s in international relations and administrative law or when placed in domestic settings, as a top feature of the ambitious open government initiative of President Obama.[68] It is argued that the modern turn to transparency dates back to "the 1950s, 1960s, and 1970s—well before the Internet—as reform-oriented

[65] *Supra* note 27.

[66] Jane R. Bambauer, Is Data Speech?, 66 STAN. L. REV. 57 (arguing that since the First Amendment protects the right to create knowledge, data is speech; if accepted, such an understanding makes any ban on data collection constitutionally suspicious).

[67] Found in the famous '*Buon Governo-Mal Governo*' 1338-9 fresco paintings of Lorenzetti in a room of Palazzio Publico in Siena, Italy, the allegory of good governance has traveled across time from Aristotle's *Politics* to 17th-18th century German economists to present-day United Nations policy documents, *see* Hans-Jürgen Wagener, "Good Governance, Welfare and Transformation", 1 THE EUR. J. OF COMP. ECON. 127 (2004).

[68] For the administration's wide-ranging number of initiatives in this respect, *see* https://www.whitehouse.gov/open/about.

politicians, journalists, watchdog groups, and social movements gained new leverage."[69] Transparency is promoted throughout a wide range of contexts but when it comes to regulation, there is little attempt to critically parcel out the different components that make up for transparency as an umbrella concept.[70] When is sunlight the "best disinfectant"[71] and when is it a mere first step to achieving a desired outcome?

In the context of holding the government to account, transparency-as-accountability has served its purpose well. The Freedom of Information Act (FOIA)[72], first enacted in 1966 and amended several times since then, applies to federal executive agencies. It creates "a judicially enforceable policy that favors a general philosophy of full disclosure based on democratic political theory and a philosophy of open government".[73] Under FOIA, numerous requests are been made by public interest organizations and law clinics that pursue surveillance reform and defend consumer privacy rights. The transmission belt that FOIA offers is premised on the idea that the pressure on the government that public debate creates as a result from the disclosures will translate into corrective measures. However, as the revelations of whistleblowers show, at the outer boundaries of the FOIA model lies the realization that we cannot request information of whose existence we simply don't know.

When it comes to the private sector, users and consumers are often unaware of the degree to which their personal information is collected and processed by companies they engage with. At first glance, it would seem that transparency-as-disclosure to consumers is a sensible regulatory strategy. The definition of informational or data privacy as the ability to determine for yourself what others may collect and how they use your information[74] has entrenched a model of privacy-as-control, which in turn brought the pervasiveness of a Notice and Choice model for regulating consumer privacy in the US. There is no generally applicable US federal privacy law that mandates privacy statements. Several sectoral laws require different degrees of disclosure on how personal information is collected and used,[75] and so do

---

[69] MICHAEL SCHUDSON, THE RISE OF THE RIGHT TO KNOW: POLITICS AND THE CULTURE OF TRANSPARENCY 1945-1975, (2015).

[70] Natali Helberger, Form Matters: Informing Consumers Effectively, Amsterdam Law School Research Paper 2013–71 (2013), available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2354988 (pointing out that our first regulatory grasp is to transparency but there is little consideration of where it works and where it does not).

[71] Louis D. Brandeis, Other People's Money and How the Bankers Use It, Frederick A. Stokes Company: New York (1914).

[72] 5 U.S.C. § 552 (1989).

[73] Michael Hoefges, Martin E. Halstuk, Bill F. Chamberlin, Privacy Rights Versus FOIA Disclosure Policy: The "Uses and Effects" Double Standard in Access to Personally Identifiable Information in Government Records, 12 WM. & MARY BILL RTS. J. 1 (despite FOIA's successes, the authors insist for a narrower interpretation of the statute's privacy exceptions when the information is in the public interest).

[74] ALAN WESTIN, PRIVACY AND FREEDOM 7 (Atheneum, 1967). For a critique, *see* Chris Jay Hoofnagle & Jennifer M. Urban, Alan Westin's Privacy Homo Economicus, 49 WAKE FOREST L. REV. 261 (2014).

[75] The Children's Online Privacy Protection Act (COPPA) mandates that websites or online services that are directed toward or knowingly collect the personal information of children under the age of 13 years, give a privacy notice. 15 U.S.C. §§ 6501–6506 (Pub.L. 105–277, 112 Stat. 2681-728, enacted October 21, 1998), implementing regulations at 16 CFR Part 312.

a number of state privacy laws.[76] The Notice and Choice paradigm has been traditionally oriented toward the individual consumer who is supposed, after reading and sufficiently comprehending the terms and conditions of the Notice, to act upon it by choosing to give or withdraw their consent (and therefore, exercise choice). However, the empirical benefits of consumer disclosure are increasingly disputed and indeed seem to be limited. First, at the core of the model sits an inherent tension between the length and accuracy of privacy notices.[77] Second, and equally problematic, there is the fallacy of consumers' "free" choice that can arise from a lack of market options but is also attributed to the set of "usual suspects": limited rationality, information asymmetries and collective action problems.[78]

1. The Limits of Transparency-as-Accountability

As Frank Pasquale has persuasively argued, when we enter the domain of Big Data, there is an ironic mismatch between the ever-growing secrecy of companies regarding their business conduct and an ever-greater quantification of individuals by these very same companies.[79] The ways in which data collection and processing are accomplished are opaque and exclusive.[80] To counter the hermetic tendencies inherent to data mining, Citron and Pasquale have called for greater transparency in algorithmic decision-making[81] as well as for interactive modeling.[82] While this proposal would certainly enhance oversight over data mining and shed light on otherwise obscure data processing practices, companies' sharing of code and models with the greater public has three key disadvantages. First, the intricacies of data mining are often the most precious resource for the industry; a transparency requirement would therefore not only threaten companies' business model but might be opposed on the ground of hampering innovation in the sector. Second, making publicly available the factors crucial for certain scoring techniques might provide opportunities for those scored to act strategically, i.e., to send artificial or exaggerated signals about the most important factors in a model. They might thus essentially "game the system".[83] This is not only well-documented by

[76] A prominent example, the California Online Privacy Protection Act (CalOPPA) requires that any website or online service that collects personally identifiable information from California residents, as defined by California law, posts its privacy policy. The actual scope of the statute is broader since it applies to any website to which Californians have provided their data, *see* California Business and Professions Code § 22575(a).

[77] Helen Nissenbaum, A Contextual Approach to Privacy Online, 140 DÆDALUS 32, 36 (2011) argues that: "[a]chieving transparency means conveying information…[however] if notice . . . finely details every [relevant fact] . . . we know that it is unlikely to be understood, let alone read. But summarizing practices in the style of, say, nutrition labels is no more helpful because it drains away important details, ones that are likely to make a difference"). The use of vague and indeterminate language in privacy notices is another persistent issue.

[78] For a poignant early critique, *see* Paul Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 825 (2000).

[79] *Supra* note 2, Pasquale (2015). *See* also Neil M. Richards & Jonathan H. King, *Three Paradoxes of Big Data*, 66 STAN. L. REV. ONLINE 41, 42 (2014). In the words of the authors, "[w]hile Big Data pervasively collects all manner of private information, the operations of Big Data itself are almost entirely shrouded in legal and commercial secrecy".

[80] Citron & Pasquale, *supra* note 2, at 17; PASQUALE, *supra* note 66.

[81] Citron & Pasquale, *supra* note 2, at 26; PASQUALE, *supra* note 79, at 16 and Chapter 5.

[82] Citron & Pasquale, *supra* note 2, at 28-29.

[83] *Cf.* Citron & Pasquale, *supra* note 2, at 20, 26 (noting, however, that in some areas gaming may be difficult to achieve).

research on search engine optimization,[84] but also more generally by economic signaling theory.[85] Third, the complexity of advanced algorithms is so great that their architecture design is often hard to fully comprehend, even by the computer scientists who contribute to algorithmic development.[86] This is a result of the collaborative dimension of generating code whereby different tech engineers contribute different pieces at different moments in time. Finally, making behavioral algorithms understandable to the wider public would be a daunting enterprise.[87]

Potentially, transparency-as-accountability can work in the area of Big Data as consumer groups, academics or regulatory bodies can exercise pressure[88] so that businesses embed algorithms that are not prejudicial to racial or other minorities. The success stories are still few and far between, however, and not hugely impressive at that. Disclosure has arguably been effective to some extent in other areas of privacy concern, such as dealing with data security breaches.[89] Perhaps if reputational damage can nudge companies into changing their practices in some areas, it can also do the trick when it comes to Big Data. One (modest) example is Facebook's changed default settings of geo-location on Facebook Messenger after a researcher put into place a browser application that publicized the scope of geo-location data collection that Facebook effectuated through its initial default setting.[90] However, the relative obscurity of technology hides away personalization from end users and watchdogs alike, limiting their ability to object to (or express any opinion on) how individuals are steered around the Web. If alternatively, code is shared only with supervisory authorities, control over one's data is put solely into the hands of a regulatory agency, something that contradicts the long-lasting perception in the US of privacy-as-control and the influential rhetoric of putting individuals back into the driver seat concerning their data. Ultimately, much like with the limitations of transparency-as-accountability under FOIA, the main problem with transparency-as-accountability in the context of Big Data remains the lack of information on the way algorithms are fueled.

---

[84] Jakub Zilincan, Search Engine Optimization, CBU INTERNATIONAL CONFERENCE PROCEEDINGS (2015), *available at* journals.cz/index.php/CBUConference2013/article/download/645/599; Amy van Looy, *Serach Engine Optimization*, *in* SOCIAL MEDIA MANAGEMENT 113 (id., ed., 2016).

[85] Howard Beales, Richard Craswell & Steven C. Salop, The Efficient Regulation of Consumer Information, 24 J. LAW & ECON. 491, 511 (1981) (noting that the signaling party will focus unilaterally on enhancing the signal and neglect other dimensions of product quality which are harder to monitor).

[86] Cf. PASQUALE, *supra* note 79, at 6.

[87] While daunting, the project is certainly not impossible, at least on the long run. An informed minority could potentially exert a disciplining influence, see Alan Schwartz & Louis L. Wilde, *Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis*, 127 U. PA. L. REV. 630 (1979); Citron and Pasquale suggest that the "[Federal Trade Commission] FTCs expert technologists" could represent such a minority, equipped furthermore with supervisory powers: Citron & Pasquale, *supra* note 2, at 25.

[88] The public's inability to comment on obscure source code has been said to obstruct the effectiveness of Privacy Impact Assessments under the E-Government Act, *see* Citron & Pasquale, *supra* note 2, at 10-11.

[89] Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, (2007).

[90] Aran Khanna, Facebook's Privacy Incident Response: A Study of Geolocation sharing on Facebook Messenger, TECHNOLOGY SCIENCE (2015).

2. The Limits of Transparency-as-Consumer-Disclosure

The key issue with consumer disclosure is that in order for it to unfold its magic a sufficient number of market participants needs to read, understand, and act upon the disclosed information. To begin with, it is important to understand that even according to traditional regulatory theory, not everyone needs to read the notice. An informed minority can exert disciplining influence on the better-informed market participants.[91] However, the informed minority hypothesis has increasingly come under attack. On the one hand, Florencia Marotta-Wurgler and others have shown in a series of papers that in the case of end-user license agreements (EULAs), virtually no one takes the time to screen the agreements for surprising or exploitative terms.[92] The authors of the studies conclude that an informed minority does not exist, at least with respect to EULAs. Similarly, in their much-discussed work on the limits of disclosure Lauren Willis and Margaret Radin have powerfully argued that the systemic neglect of disclosure is a rampant phenomenon in many other markets as well.[93] On the other hand, even if an informed minority does exist in some markets (such as arguably with institutional investors in financial markets),[94] the personalization effect of Big Data increasingly enables providers to discriminate between better and less informed customers so that the spillover effects of the presumed informed minority get substantially limited. More importantly, Big Data would be able to identify loyalty: a loyal customer is one who does not compare shops and thus, there would be no reason for businesses to offer better prices to the loyal customer.

In response to critics, legal scholars have recently called for cognitively optimizing disclosure. "Smart" disclosures use multilayered formats, graphic explanations, images, traffic lights and symbols.[95] However, as empirically proven by Alessandro Acquisti and others,

---

[91] See *supra* note 74, Alan Schwartz & Louis L. Wilde; David M. Grether, Alan Schwartz & Louis L. Wilde, *The Irrelevance of Information Overload: An Analysis of Search and Disclosure*, 59 S. CALIF. L. REV. 277 (1986).

[92] Florencia Marotta-Wurgler, Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts", 78 U. CHI. L. REV. 165 (2011); Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts, 43 J. LEG. STUD. 1 (2014).

[93] Lauren E. Willis, Decisionmaking and the Limits of Disclosure: The Problem of Predatory Lending: Price, MD. L. REV., Vol. 65, 2006 and Lauren E. Willis, Against Financial Literacy Education, IOWA L. REV., Vol. 94, 2008 (arguing further that the attempt to educate consumers on financial matters in order to improve the workability of disclosure is untenable at best); MARGARET J. RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2013) (demonstrating how the use of boilerplate language in disclosure has degraded traditional notions of consent and contract, and sacrificed core rights whose loss threatens the democratic order); *See also* OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW. THE FAILURE OF MANDATED DISCLOSURE (2014).

[94] *See, e.g.*, STEFAN GRUNDMANN, EUROPEAN COMPANY LAW. ORGANIZATION, FINANCE AND CAPITAL MARKETS, § 9: DISCLOSURE (2012).

[95] Calo supra note 14; Richard H. Thaler & Will Tucker, Smarter Information, Smarter Consumers, HARV. BUS. REV. 3 (January-February 2013); Philipp Hacker, Nudge 2.0 – The Future of Behavioural Analysis of Law, in Europe and Beyond. A Review of 'Nudge and the Law. A European Perspective', Edited by Alberto Alemanno and Anne-Lise Sibony, EUROPEAN REVIEW OF PRIVATE LAW (forthcoming), available at http://ssrn.com/abstract=2670772, at 20.

people tend to perceive the disclosure as a "seal".[96] Further, in a recent paper Omri Ben-Shahar and Adam Chilton have found that the most often recommended strategies for simplifying disclosure did not have an effect on addressees – in fact, disclosees chose to equally ignore standard and cognitively optimized disclosures.[97] This study is particularly pertinent to the prospect of using smart disclosure techniques in the realm of Big Data since the authors manipulated the design of privacy notices in what concerns an area of particularly sensitive information – sexual practices. Despite the fact that highly intimate data was concerned, the participants in the study took only an average of 19 seconds to look at the cognitively optimized privacy notice and only an average of 13 seconds for the standard version.[98] The cognitive optimization of disclosures can in fact be useful once people start reading the notice.[99] However, the potential of disclosure remains limited first and foremost because of the limited motivation individuals have to attend to the disclosed information.[100] At least in the domain of Big Data, where we have shown that the stakes are critical for the life of the individuals concerned, the results of Omri Ben-Shahar and Adam Chilton[101] should be a cautionary note for those striving to achieve ever better salience in privacy notices. Instead, we suggest coupling disclosure techniques that rely on the privacy-as-control paradigm with more substantial types of regulation.

B. Substantial Regulation

The most obvious way to tackle issues of discrimination by means of substantial regulation is antidiscrimination law. However, traditional antidiscrimination law, as Solon Barocas and Andrew Selbst have convincingly shown,[102] is unable to cope with data-driven forms of discrimination. As we have noted above, this chiefly results from the difficulty to square the doctrine of disparate impact with discrimination hidden in "dual-valence" correlations and "smart discrimination".[103] Therefore, we turn to novel tools, which aim to give citizens greater control over their data in the first place. With this lever, we hope to mitigate legal inequality, not through remedying and controlling disparate impact, but through substantially decreasing access to data on which data-driven discrimination can be built. As a second step, we inquire into the potential of actively using Big Data in regulation to combat economic and legal inequality.

---

[96] Idris Adjerid, Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Sleights of Privacy: Framing, Disclosures and the Limits of Transparency*, (2013) Symposium on Usable Privacy and Security (SOUPS), Newcastle, UK.

[97] Omri Ben-Shahar & Adam S. Chilton, *Simplification of Privacy Disclosures: An Experimental Test*, Working Paper (2016), available at http://ssrn.com/abstract=2711474.

[98] Ben-Shahar & Chilton, *supra* note 97, at 14 and Supplementary Material, at 17. Since the notices contained between 500 and 900 words and since an average reader can read about 300 words per minute, it can be inferred that the participants were not motivated enough – despite the high stakes of collection of intimate information – to read, let alone cognitively digest the disclosures (*id*., at 22).

[99] Nick Chater, Steffen Huck & Roman Inderst, Consumer Decision-Making in Retail Investment Services: A Behavioral Economics Perspective. Final Report 336-37 (November 2010), *available at* www.vse-lee.cz/files/useruploads/eu_consumer_behaviour_final_report.pdf.

[100] *See* Adrian Weser, *Die informative Warenkennzeichnung* [Informational Leaflets for Goods], J. CONS. POL'Y 80, 85 (reporting a Swedish field study according to which only 3 % of participants evaluated furniture in a department store according to information leaflets attached to the furniture).

[101] Ben-Shahar & Chilton, *supra* note 84.

[102] Barocas & Selbst, *supra* note 4.

[103] *Supra*, Part I.1.

Substantial regulation can take a variety of forms and draw on a large number of regulatory tools ranging from soft paternalistic nudges to full-blown mandates. In this piece, we will advance four proposals that seem particularly helpful in tackling the challenges of lack of transparency and the rising inequality provoked by smart discrimination and dual valence correlations. Our proposals are: mandatory active choice between payment with money and payment with data, ex post evaluation of privacy notices, democratized data collection, and wealth or income-responsive fines. While other valuable proposals have been put on the table,[104] we enrich and broaden the debate by introducing four novel categories.

1. Toward a Real Choice between Payment with Money and Payment with Data: Forcing Data Free Services

The first option consists in mandating an active choice by consumers and users about whether to pay for an online service indirectly through their data or directly through monetary payments. This gives citizens an "exit strategy" from data collection. As known, data collection services such as Facebook create psychographic profiles on people and infer hidden data (such as race, sexual orientation) from preference data for advertising purposes. But Facebook and others have other plans on how to monetize this data in surprising ways: the Facebook app could be used for all sorts of other decisions, such as authentication, security checks, even controlling car traffic flow.[105] Beyond targeted advertising therefore, some Facebook-generated data might be used in areas, which potentially have much greater impact on the individual and where the risk for discrimination is higher. The vulnerable car buyer or the prospective non-white tenant from our examples in Section 1 might feel that they are more likely to be subjected to discrimination by Facebook and therefore, decide to opt for a data-free service.

The reason for a regulatory intervention in the market by a mandatory active choice regime is twofold. First, as was noted,[106] the attitude-action gap in the domain of privacy protection by online users points to a lack of meaningful choice concerning data-protecting alternatives to data-collecting services. Given the potential use of data in a wide range of areas which include those with a high potential for discrimination, such as housing or labor markets, increasing the offer or the salience of alternative, data-free services seems crucial. Moreover, even for users who are currently aware of privacy-respecting alternatives such as the few providers offering messaging services in exchange for monetary instead of data compensation, the lock-in or network effect mentioned above will often make a switch to these alternatives unattractive.[107] What is the use of joining a messaging service or a social

---

[104] Citron & Pasquale, *supra* note 2, at 22-28; VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA. A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 171–84 (2014); Barocas & Selbst, *supra* note 4, at 46-59; Sara Hajian, Josep Domingo-Ferrer, *Direct and Indirect Discrimination Prevention Methods*, *in* DISCRIMINATION AND PRIVACY IN THE INFORMATION SOCIETY 241 (Bart Custers, Toon Calders, Bart Schermer, and Tal Zarsky eds., 2013); for technical proposals based on discrimination-free classifications, see Calders & Verwer, *supra* note 35; Faisal Kamiran, Toon Calders & Mykola Pechenizkiy, *Techniques for Discrimination-Free Predictive Models*, *in* DISCRIMINATION AND PRIVACY IN THE INFORMATION SOCIETY 223 (Bart Custers, Toon Calders, Bart Schermer, and Tal Zarsky eds., 2013).

[105] We are grateful to Chris Hoofnagle for pressing us on this point.

[106] *Supra*, notes 20-24 and accompanying text.

[107] For an account of network effects in the digital economy, see ROBERT H. FRANK & PHILIP J. COOK, THE WINNER-TAKE-ALL SOCIETY (1995); Yifan Dou, Marius F. Niculescu & D. J. Wu, *Engineering Optimal*

network if most of my friends cannot be reached within it? Therefore, it seems more promising to require in particular the big players to offer data-free services rather than to expect the market to self-correct. Whereas such a regulatory tool might endanger the business model of a small start-up that would be hesitant to introduce a data-free option, big companies like Facebook and Google already have a large pool of data due to the many users they have. Therefore, such companies can first implement our proposal in a pilot version. Again, the existing vast attitude-action gap suggests that market-based self-correction strategies are currently not working properly.

While proposals have already been made in the direction of considering the monetary effect of "free" services,[108] we add to the existing literature in three distinct ways: first, we frame the decision between data-collecting and data free-services as an instantiation of "active choice", a technique analyzed extensively in the behavioral scholarship. This allows us to uncover the necessary conditions for this mechanism to function adequately. Second, we provide a concrete estimate for the possible price range of the paid compared with the data free option, streamlining the debate on the monetization of "free" services and the economic value of data.[109] Third, we offer an analysis of the crucial question of price control for the data-free option.

The proposal thus draws on a technique popularized by behavioral law and economics, i.e., active choice.[110] The key idea would be to force providers of so far "gratuitous" services to offer users a clear choice between two different contracts. Under the first option, users would not be required to make any monetary payments and the providers would be allowed to collect and process their data in return for services, as is now the case with Google, Facebook, Microsoft Hotmail and others (the data-collecting option). Under the second option, users would make monetary payments (be it on a one-off basis for each service or on a monthly basis) and providers would not be allowed to collect or process any of the users' data (the data-free option).[111] Every provider of online services would thus be required to present at

---

Network Effects via Social Media Features and Seeding in Markets for Digital Goods and Services, 24 INFORMATION SYSTEMS RESEARCH 164 (2013); Jeffrey Church & Neil Gandal, *Network Effects, Software Provision, and Standardization*, 40 J. INDUSTRIAL ECON. 85, 86-87 (1992).

[108] *See, e.g.*, the swift discussion in Calo, *supra* note 7, at 1047-48; more substantially, Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV 606 (2014), at 661-62 (explaining that "free" services actually state a price for their services and that their users should be treated as consumers for the purposes of consumer protection law); *see also* Henk Kox, Bas Straathof & Gijsbert Zwart, *Targeted advertising, platform competition and privacy*, CPB Discussion Paper 280 (July 1, 2014), available at http://www.cpb.nl/en/publication/targeted-advertising-platform-competition-and-privacy.

[109] *See* Arslan Aziz & Rahul Telang, *What Is a Digital Cookie Worth?* Working Paper (March 31, 2016), available at http://ssrn.com/abstract=2757325; Hoofnagle & Whittington, *supra* note 108, at 634-640 and 666-667.

[110] Cass R., Sunstein & Richard H. Thaler, *Libertarian Paternalism is not an Oxymoron*, 70 U. CHI. L. REV. 1159, 1173 (2003); Cass R. Sunstein, *Empirically Informed Regulation*, 78 U. CHI. L. REV. 1349, 1400 (2011); CASS R. SUNSTEIN, CHOOSING NOT TO CHOOSE. UNDERSTANDING THE VALUE OF CHOICE (2015).

[111] Hoofnagle & Whittington, *supra* note 108, at 669-70 note that such a contract does not guarantee that data is not collected illegally; however, they also observe that it can mark the transition from a "free" to a "paid" service space, in which, we suggest, the collection practices of the paid part should be supervised closely to minimize illegal conduct. In this domain, the suggestion for the establishment of an independent supervisory

least one data-free option for every service it publicly offers on the market. As Henk Kox, Bas Straathof and Gijsbert Zwart have demonstrated, such a segmented market structure would maximize both consumer and total surplus, particularly if consumers have heterogeneous preferences with respect to privacy and tracking.[112]

Mandating an active choice between these two sets of options only makes sense, however, if it can be expected to make a difference in user choice. Recent scholarship has identified two key conditions that should hold in order for active choice to be effective. First, fairly large heterogeneity in actor preferences between the two choice options must be expected. The reason for this is that, if actor preferences tend to be homogenous, a default rule tailored toward these preferences will often be more effective and potentially less intrusive. However, in agreement with other scholars,[113] we expect preferences of users to diverge heavily on the question of whether they are willing to pay with money instead of with data. The issue of data protection and privacy polarizes society and legal discourse as few other issues do, which is why an assumption of rather uniform preferences can be safely rejected. The charm of active choice is that users will be able to sort themselves into categories depending on their respective preferences.

Second, users should be expected to be in a position to make a meaningful choice between the two options. More specifically, they should be better able to make that choice than a regulator (crafting a default rule or a substantial mandatory provision). For this condition to be fulfilled, it seems clear that additional information needs to be given to consumers to demonstrate what is at stake in the choice between the data-collection and the data-free option. Many users at the moment seem to be unaware of the fact that they are indirectly paying for "gratuitous" services with their data. The most salient way to enable a comparison between the two options would therefore be to attach a monetary price tag on both. While this is simple to calculate for the data free-option, where a monetary payment has to be made anyway, it is more difficult to estimate the value given away by the consent to collect and process user data. Nevertheless, the salience of the monetary consequences of choice seems crucial: in other areas of consumer choice, empirical studies suggest that the most effective notices are those highlighting the monetary consequences for consumers.[114]

What could be a good proxy for the value of user data? We use two estimation strategies: a bottom-up and a top-down one, and test the results against the results of a recent study.[115] First, an average lower threshold for the value of user data can be constructed by comparing the prices providers can charge for personalized and for non-personalized advertising, respectively (bottom-up approach). According to industry sources, companies can

---

authority is worthwhile, see Andrew Tutt, *An FDA for Algorithms*, Working Paper (March 15, 2016), available at http://ssrn.com/abstract=2747994.

[112] Henk Kox, Bas Straathof & Gijsbert Zwart, *supra* note 108, at 5 (modeling significant positive externalities from low privacy to high privacy-sensitive consumers in a competitive framework).

[113] Henk Kox, Bas Straathof & Gijsbert Zwart, *supra* note 108, at 7.

[114] Richard G. Newell & Juha Siikamäki, *Nudging Energy Efficiency Behavior: The Role of Information Labels*, 1 J. ASSOCIATION ENVIRONMENTAL & RESOURCE ECONOMISTS 555, 593 (2014); Cristiano Codagnone, Francesco Bogliacino & Giuseppe Veltri, *Testing CO2/Car labelling options and consumer information*, Final Report (2013), available at http://ec.europa.eu/clima/policies/transport/vehicles/labelling/studies_en.htm, at 9.

[115] Aziz & Telang, *supra* note 109.

charge roughly 10 times more for personalized advertising (retargeting) vis-à-vis standard advertising. According to the same sources, 1000 personalized advertisements on Facebook mobile would cost approximately 50 cents, and about twice the amount for the desktop version of Facebook. Thus, each personalized advertisement costs between 0.1 and 0.05 cents. Let us further assume that the average user sees 100 advertisements per day (a generous estimate). The revenue from personalized advertising for a single average customer thus lies between 5 and 10 cents per day, or between $1.50 and $3 per month. In a conservative estimate, we can therefore say that the difference between personalized and non-personalized advertising in the case of Facebook for a single average customer amounts to roughly $2.70. We have to add to this the indirect revenue that Facebook, and other companies, generate through personalizing advertisements on websites of third parties by using Facebook's, or other companies', own data. This "audience network" is a growing source of revenue in the industry. Average revenue from third-party websites is very difficult to ascertain, however a total spread between personalized and non-personalized advertising of roughly $4 per month should be a good estimate. For an average user this sum represents an estimate of the total marginal value of permitting versus not permitting the collection of user data. At the same time, it offers a glimpse of where a competitive price for a data-free service might stand. While some degree of uncertainty remains, it seems highly plausible to assume that at least the dimension (ranging $1 to $10) is correct.

This finding is corroborated by an estimate using a different calculation strategy: comparing the total revenue of Facebook with the total number of users (top-down approach). For the fiscal year of 2015, total revenue stands at $17.93 billion per year,[116] the most significant part of this being revenue from advertising. As of the last quarter of 2015, the total number of users was 1.59 billion.[117] Thus, Facebook generates an average of about ten dollars of revenue from advertising per user per year, or about one dollar per month. Between the two results of the bottom-up ($4 per month) and the top-down approach ($1 per month), we choose the one with a higher estimate since data collected today most likely will have a significant number of uses in the future which we could not take account of in our estimates.

This result is further strengthened by the results of a recent empirical study. The authors have used a large dataset of individual bid-level data points from real-time retargeting auctions to empirically determine the effectiveness of personalized advertisements (or, in the jargon of the industry: (re)targeting[118]). They found that more personalization generates better predictions concerning the user's value, i.e., it is instrumental in estimating their purchase probability, but at a diminishing rate.[119] In this way, it also makes advertisements more effective, since advertisements tend to exhibit greater influence on purchasers who have a higher probability of buying in the first place. [120] These, in turn, can be identified with the aid of data technologies such as digital cookies. Finally, Aziz and Telang calculate a dollar

[116] http://www.marketwatch.com/investing/stock/fb/financials,

[117] http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

[118] Retargeting is the practice of targeting consumers who have already been in contact with a company or a product, see Aziz & Telang, *supra* note 109, at 4.

[119] Aziz & Telang, *supra* note 109, at 9.

[120] Aziz & Telang, *supra* note 109, at 24-25.

amount of the marginal value of personalized ads: $1.7 Billion per quarter in the US across the entire economy.[121] In 2015, 205 million US citizens were qualified as online shoppers.[122] This corresponds to a marginal value of roughly $2.8 per US online shopper per month for personalized ads.[123] This number covers all e-commerce, not only one company. However, since Facebook is one of the largest users of cookies and personalized ads,[124] we can estimate that a large fraction of this number corresponds to the marginal value for Facebook. Thus, again, the prize for the data-free option lies within our estimated range of $1-10 per month.

Both options, the data-collecting and the data-free, would therefore have to feature a prominent, salient notice, which could read, for the former:

> **"For this option, you pay with your data. An average user gives away monthly data worth about $4."**

For the data free option, the notice could read:

> **"For this option, you pay with your money instead of your data. The monthly price is $[x]."**

The two major agencies involved in enforcing privacy policies, the Consumer Financial Protection Bureau (CFPB) or the Federal Trade Commission (FTC), could develop concrete guidelines for the framing of the notice. At least from a normative vantage point, the rules should also be constitutional, even in the light of the compelled commercial speech doctrine of the Supreme Court.[125]

A final problem with this proposal, however, is that its effectiveness crucially depends on the price companies would charge for the data-free service. What would prevent companies who would like to thwart efforts to change their business model from charging prohibitive prices for the data-free option, such as $100 for a month of Facebook's use?[126] Such strategies would particularly make data-free services unavailable for low-income people, adding to economic inequality. Since many data-services generate considerable network (lock-in) effects, it will not be enough to simply rely on competition in order to drive down prices.[127] All efforts to constrain the freedom of a company to charge what it deems to be a competitive price for the data-free option, however, enter the treacherous terrain of price control by the state. Arguably, the most one could hope for is the enforcement of a provision stating that the price of the data free-service must be reasonable in comparison with some

---

[121] Aziz & Telang, *supra* note 109, at 30; in fact, this is the marginal value resulting from allowing most conventional tracking vis-à-vis only allowing the tracking of the type of browser a user uses.

[122] http://www.statista.com/statistics/183755/number-of-us-internet-shoppers-since-2009/

[123] The actual amount is likely to be higher since Aziz and Telang's baseline is minimum targeting, not zero targeting, see *supra* note 121.

[124] *Cf.* Brandon Workman & Emily Adler, *Facebook Is Emerging As A Huge Engine For Driving E-Commerce Traffic And Purchases*, Business Insider (Nov. 14, 2014), available at http://www.businessinsider.com/how-facebook-drive-e-commerce-sales-2014-10?IR=T; *cf. also* https://www.shopify.com/blog/12731545-which-social-media-platforms-drive-the-most-sales-infographic

[125] *See* Christine Jolls, *Debiasing Through Law and the First Amendment*, STAN. L. REV. (forthcoming); *cf. further* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1035-40 (2014).

[126] *Cf.* Hoofnagle & Whittington, *supra* note 108, at 662.

[127] *Cf.* Pasquale, *supra* note 79, at 141; *see also supra*, note 107.

benchmark. Antitrust law provides some examples of how such a strategy could be given meaning. A classical problem of antitrust under § 2 Sherman Act is predatory pricing, i.e., pricing a good below marginal cost in order to hurt competitors.[128] In order to determine whether predatory pricing occurs, one strategy is to compare prices with actual marginal cost. While predatory pricing occurs when the prices are *below* marginal cost, conscious deterrence of users from the data-free option would require pricing significantly *above* marginal cost. Thus, the feasibility of enforcement hinges on the approximate determination of actual marginal cost. As antitrust scholars Areeda and Turner have suggested, average variable cost[129] can be used as a proxy for marginal cost.[130] Data on the former is usually much more readily available than for the latter.[131] The test is thus widely used, with some variations, by courts both in the US and in the European Union (EU).[132] We therefore suggest an "inverse predatory pricing approach" using the average variable price test in order to determine whether the actual price charged is reasonable.

Moreover, there is a second proxy that can be used to determine the reasonableness of the price of the data free-option: the marginal value of data given away in the data-collection option. The direct payment in the data-free option is introduced precisely to make up for losses generated by the impossibility of marketing data under this contract. Therefore, the marginal value of personalized data as calculated above can provide a benchmark for measuring whether prices are too high.

The final problem is that the number of people using the data-free service might dynamically affect the marginal value. Generally, if as a consequence of the active choice regime the total amount of user data available to the provider shrinks, the amount of training data and hence, the predictive quality of algorithms will be reduced. Less predictive power, however, means less marginal value. The opt-out of data sensitive users therefore can be expected to have spillover effects on the value of the data of those users that will retain the data-collecting option. However, this does not disqualify our proposal: If the data-free option

---

[128] Phillip Areeda & Donald F. Turner, Predatory Pricing and Related Practices under Section 2 of the Sherman Act, 88 HARV. L. REV. 697, 702 (1975); Nicola Giocoli, When low is no good: Predatory pricing and U.S. antitrust law (1950–1980), 18 EUR. J. HISTORY ECON. THOUGHT 777, 780-83 (2011).

[129] For a useful definition of average variable cost, see Phillip Areeda & Donald F. Turner, *Predatory Pricing and Related Practices under Section 2 of the Sherman Act*, 88 HARV. L. REV. 697, 700 (1975) ("Variable costs, as the name implies, are costs that vary with changes in output. They typically include such items as materials, fuel, labor directly used to produce the product, indirect labor such as foremen, clerks, and custodial help, utilities, repair and maintenance, and per unit royalties and license fees. The average variable cost is the sum of all variable costs divided by output.")

[130] Phillip Areeda & Donald F. Turner, *Predatory Pricing and Related Practices under Section 2 of the Sherman Act*, 88 HARV. L. REV. 697, 716-18, 733 (1975); see also William J. Baumol, *Predation and the Logic of the Average Variable Cost Test*, 39 J L. & ECON. 49 (1996).

[131] Phillip Areeda & Donald F. Turner, *Predatory Pricing and Related Practices under Section 2 of the Sherman Act*, 88 HARV. L. REV. 697, 716 (1975); Nicola Giocoli, *When low is no good: Predatory pricing and U.S. antitrust law (1950–1980)*, 18 EUR. J. HISTORY ECON. THOUGHT 777, 795-96 (2011).

[132] *See* William J. Baumol, *Predation and the Logic of the Average Variable Cost Test*, 39 J L. & ECON. 49, 49 (1996); Christopher R. Leslie, *Predatory Pricing and Recoupment*, 113 COL. L. REV. 1695, 1701 (2013); Aaron Edlin, *Predatory Pricing*, *in* RESEARCH HANDBOOK ON THE ECONOMICS OF ANTITRUST LAW (Einer Elhauge ed., 2012).

is chosen only by a minority of users, it won't affect the marginal value of the remaining users' data by much. If it is chosen more often, and the marginal value is negatively impacted, the company is always free to demonstrate that the marginal value has decreased, and to adapt the notice and pricing accordingly.[133] Furthermore, our proposal can be tested in a pilot phase.

To conclude, the price should be deemed unreasonable if it is more than 1.5 times of either average variable cost or the marginal value of personalized data. The enforcement of such a reasonableness requirement could be left to anti-trust authorities such as the FTC, which has considerable experience with predatory pricing. It would provide the necessary bite for a mandatory data-free option to be implemented within a scheme of active choice.

The advantages of a scheme of active choice are clear. First, it enhances transparency by saliently uncovering that users are indirectly paying for "free" services with their personal data. Second, it remedies another key flaw inherent in the current disclosure mechanism: the lack of meaningful choice. Many services today are offered on a take-it-or-leave-it basis. For services offered by dominant companies such as Facebook or Google, often there is no meaningful, equally satisfying alternative. Due to network (lock-in) effects, even for users who would prefer not to share their data *but* remain on Facebook, there is no available alternative. Mandating an active choice, and thus mandating a data-free service, puts the user back in control over whether she wants to share or not data with the company in the first place

In this section, we have argued that to the extent that data are shared less the technique of active choice reduces the potential for discrimination for the most vulnerable groups. It is particularly noteworthy that users who fear potential discrimination could choose a data-free option. Since discrimination can take place along a range of different characteristics, ranging from sexual orientation to racial or social background to political affiliations, it is also unlikely that the choice of the data-free option will become a signal of belonging to any specific minority group (which in turn could invite discrimination against the users of a data-free service). Rather, it is to be expected that the option will be selected for a wide variety of motives, from fear of discrimination by potentially vulnerable individuals all the way to the conscious refusal of some consumers to share their personal data as a matter of principle. These are legitimate motives worthy of being supported by legal means. Price control by an inverse predatory pricing strategy, as suggested here, ensures that even low-income users get access to data-free services, thus incrementally contributing to mitigating economic inequality. Finally, we have shown that introducing a data-free (paid by money) option by services powered by Big Data is unlikely to endanger the business model of major market players that can adjust pricing according to the marginal value.

2. Unconscionability and Ex Post Evaluation

An active choice between a data-collecting and a data-free option will only get us so far, however. It seems reasonable to expect that at least some less educated users will stick

[133] If it becomes apparent that the marginal value drops to an extent that a data-free service cannot be profitably maintained at a price of less than 150 % of the marginal value, the cap could be exceptionally raised by the supervisory authority, e.g. to 180 %. This would not hurt users much since the absolute price, after a drop in the marginal value, would stay approximately the same.

with the data-collecting option and would thus remain vulnerable in terms of discriminatory uses of their data. Since disclosure has proven unavailing in recent years, we suggest resorting to a more intrusive but potentially more effective remedy: ex post evaluation of the contractual validity[134] of privacy provisions, both by supervisory authorities and courts.

It is well known, however, that in the US a regime of scrutiny of unfair contractual terms by the courts is virtually inexistent.[135] The closest analogy can be found in the doctrine of unconscionability, particularly as applied by the California courts.[136] We are therefore the first to propose an analysis on how far this doctrine can be fruitfully applied to the ex post evaluation of the validity of privacy standards dictated by data processing companies.

The unconscionability doctrine generally requires the fulfillment of two elements, one procedural and one substantive. Both are necessary, but a deficiency in one can be balanced in an overall assessment by a greater weight of the other prong.[137] Case law has established that procedural unconscionability requires the absence of meaningful choice of one party to the contract.[138] This definition is corroborated by § 208 cmt. d of the Restatement (Second) of Contracts. Procedural unconscionability further presents when there is either oppression or surprise,[139] a dichotomy also highlighted by § 2-302 cmt. 1 of the Uniform Commercial Code (UCC). Oppression is found paradigmatically when there is an inequality of bargaining power, which results in the absence of negotiation and meaningful choice. More often than not, take-it-or-leave-it offers have qualified to meet the "oppression" prong of the unconscionability standard.[140] In turn, surprise is evoked when a clause is hidden in the "prolix printed form".[141] The surprise element also leads to unenforceability under § 211(3) of the Restatement (Second) of Contracts). In the realm of privacy and data protection, however, it will be difficult to find surprise given the widespread use of data collection, sharing and processing clauses. Therefore, if procedural unconscionability is to have a bearing on data privacy provisions, it must be through the oppression element.

There are two distinct problems with finding procedural unconscionability in privacy provisions. First, a broad interpretation of oppression is not shared by all districts.[142] Therefore, a solution based on these principles would apply at most to residents of California,

---

[134] For a taxonomy of algorithmic contracts, *see* Lauren H. Scholz, *Algorithmic Contracts*, STAN. TECH. L. REV., forthcoming.

[135] *See* Lewis A. Kornhauser, *Unconscionability in Standard Forms*, 64 CALIF. L. REV. 1151, 1159 (1976); Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. REV. 1203, 1204, 1255 (2003).

[136] Ian Ayres & Gregory Klass, Studies in Contract Law 548-49 (8th ed. 2012). For an analysis of California's frontrunner role and future potential on other areas of privacy law and policy development in the US, *see* Bilyana Petkova, The Safeguards of Privacy Federalism, 20: 2 LEWIS & CLARK L. REV. (2016, forthcoming).

[137] Armendariz v. Foundation Health Psychcare Services, Inc., 6 P.3d 669, 690 (Cal. 2000); Ferguson v. Countrywide Credit Industries, Inc., 298 F.3d 778 (9th Circ., 2002).

[138] Williams v. Walker-Thomas Furniture, 121 U.S. App. D.C. 315 (1965).

[139] Ferguson v. Countrywide Credit Industries, Inc., 298 F.3d 778 (9th Circ. 2002).

[140] Stirlen v. Supercuts, Inc., 60 Cal.Rptr.2d 138, 145 (Ct.App.1997); Ferguson v. Countrywide Credit Industries, Inc., 298 F.3d 778 (9th Circ., 2002); *see also* Williams v. Walker-Thomas Furniture, 121 U.S. App. D.C. 315 (1965) (holding that gross inequality of bargaining power can lead to lack of meaningful choice).

[141] Id.

[142] *Cf.* AYRES & KLASS, *supra* note 136, at 547-49.

leaving large parts of the US out of the picture. Second, as soon as the scheme of active choice described in the previous section is implemented, it will be impossible to argue that there is no meaningful choice for consumers. Therefore, unconscionability will be unhelpful for those consumers who choose the data-collecting option under the active choice regime. Nevertheless, it may still play a prominent role as long as there is no law enacting such a scheme.

Under current circumstances, it may thus be persuasively argued that there is indeed an inequality of bargaining power between data processing companies and individual users. Negotiation is fully absent from the bargaining process, take-it-or-leave-it offers are drafted by dominant firms such as Facebook or Google; these contracts leave no reasonable alternatives for potential users. It should be noted that at least in California, the option to conclude a contract with another party on more favorable terms does not hinder the finding of procedural unconscionability.[143] Therefore, under the *Ferguson* standard,[144] oppression and hence, procedural unconscionability may be found in the current practice of contractual privacy provisions.

The substantive prong is generally deemed fulfilled under *Ferguson* when the terms of the agreement are so one-sided as to shock the conscience.[145] Other formulations suggest it to be sufficient that the terms are unreasonably favorable to one party.[146] Reasonable people will disagree on what terms exactly qualify for substantive unconscionability under either standard. However, it seems plausible to assume that particularly egregious and profit-making forms of data sharing and processing confer a sufficiently unilateral advantage to data-processing companies. Examples include data shared unrestrictedly with third parties, data used to personalize advertisements not only within the scope of the actual service offered by the company but also on external websites, or when massive amounts of profit are generated from these data without users monetarily sharing in them.[147]

All in all, there is reason to believe that the application of the California doctrine of unconscionability is a way forward to invalidate the most egregious provisions of data sharing and processing. However, it falls short of providing a solution for the entire US because of its restricted geographical scope and its incompatibility with the scheme of active choice advocated in the previous section. The gold standard would certainly be to include a clause outlawing inappropriate data collection, sharing and processing in federal and state data protection laws. Such a general clause could be enforced publicly by the FTC and simultaneously privately through actions in civil courts, as is the case with existing unfair trade provisions or securities regulation. Another option would be to attach an extraterritorial element to the doctrine, much like existing legislation, such as the California Online Privacy

[143] Szetela v. Discover Bank, 118 Cal.Rptr.2d 862, 867 (Ct.App.2002)

[144] See *supra*, note 139. In *Ferguson*, the Court held that oppression can be deduced from an inequality of bargaining power which results in absence of negotiation and meaningful choice, thus making the prong applicable to take-it-or-leave-it contracts, or contracts of adhesion.

[145] Kinney v. United Healthcare Servs., Inc., 83 Cal.Rptr.2d 348, 353 (Ct.App.1999); Ferguson v. Countrywide Credit Industries, Inc., 298 F.3d 778 (9th Circ. 2002).

[146] Williams v. Walker-Thomas Furniture, 121 U.S. App. D.C. 315 (1965).

[147] *See infra* notes 180-178 for a more detailed treatment of the unconscionability of such terms.

Protection Act (CalOPPA) does for other areas of privacy concern. Finally, the current effort of the American Law Institute (ALI) to draft a new Restatement of Consumer Contracts might present another opportunity for (re)introducing unconciouability into US law.[148]

3. Democratizing Data Collection and Processing

Reconciling data collection with democratic principles and putting control over personal data back into the hands of those being tracked can be seen as a key political and legal challenge in the age of Big Data. The problems associated with policing code for the general public may be overcome in the long run, but they point to the need for further ideas about democratizing data processing and collection in the meantime.. We are advancing the following here:

Our first proposal consists in forcing (large) companies to routinely conduct representative surveys among current and potential users to determine whether users would prefer less collection and processing of their data, as well as to see the extent to which users actually understand the bargain offered by the company. Such a requirement would go well beyond the mere exhortation to develop codes of conduct, widespread in other areas of privacy law in the US and envisioned in the EU General Data Protection Regulation[149]. The surveys, while triggering only moderate immediate consequences, would enable users, including those who are potentially more prone to discrimination, to regain institutionalized voice. While an obligation to comply with the findings would probably constitute too deep an intrusion into the freedom to conduct business, companies could be required to publicly and saliently disclose the results of their survey. Thus, future business policies of the company could be measured against the results of the survey to ascertain whether companies voluntarily comply with the suggestions of their users. It can be expected that the results of the survey will exert at least a moderate disciplining influence on companies' data policies. Repeated noncompliance with the suggestions of the survey could be highlighted by activists or potentially even punished by investors.

The other option is also of an institutional nature and consists in the obligatory inclusion of a data protection compliance officer in each company to be elected partly by current users and reporting directly to the CEO of a company. The voluntary spread of the institution of a data protection officer has been generally welcomed in other areas of privacy concern and is said to have exercised a transformative influence on the generation of a culture of compliance across the US corporate sector.[150] Such a position, albeit less strictly defined, is now also envisaged in the new EU General Data Protection Regulation.[151]

---

[148] For ALI's timeframe, *see* https://www.ali.org/projects/show/consumer-contracts/

[149] Art. 40 of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. 2016, L 119/1. *See also Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S: J.L. & Pol'y for Info. Soc'y 356, 357 (2011).

[150] Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Ground. Driving Corporate Behavior in the United States and Europe (MIT, 2015).

[151] Art. 37 of Regulation 2016/679, *supra* note 148.

How could the election of such an officer by current users be operationalized? We suggest that votes are split equally between the board of directors and users. Thus, the totality of the votes of board members is weighted so as to correspond to the weight of half of all votes cast. The remaining half comes from users if the user turnout surpasses a certain threshold of, e.g., 20 %. This strategy ensures that a minority of activist users is not driving up the result of the election. However, if users do not care to read privacy notices,[152] can they be expected to cast votes for such a position at all? On the one hand, if they do not participate in sufficient numbers, the board will appoint the officer as the user vote is discounted to 0. On the other hand, making the issue of data use and collection salient and explaining that users have a chance to shape the policy and structure of the company should help install significant incentives to vote. After all, the strategies we propose here such as the publication of user surveys and mandated active choice regime can all work in conjunction to increase the salience of the issue of data collection and use by companies. The election of a data compliance officer pairs this heightened awareness with a real, institutionalized voice for consumers.

4. Wealth- or Income-Responsive Fines

Our first three suggestions were all geared toward restraining the practices of Big Data companies. Finally, we come back to our proposal on actively combatting economic and legal inequality through Big Data. In Section I we discussed not the only the negative externalities triggered by uses of Big Data but also hinted to its potential for promoting equality. In particular, we gave the example of positive price discrimination based on wealth indicators by private companies such as Amazon. However, positive price discrimination can only be a very incomplete contribution to the mitigation of economic inequality since the resulting distributional effect would channel wealth from buyers to sellers, but in all likelihood it would not reach out to the most economically disadvantaged layers of society. To rein in the potential of Big Data, we are thus suggesting a strategy of data-driven fines for both individuals and companies.

The most direct way of tackling inequality by means of Big Data is to couple administrative and criminal fines with wealth or income in a progressive way, similar to progressive income tax schemes. Such a system of what may be termed "economic affirmative action" would not necessarily run afoul of the equal protection clause of the Fourteenth Amendment since "wealth" is not a protected class within its ambit;[153] rather, as was argued in Part III, it would reinforce equality before the law. The question of whether criminal and administrative fines should depend on the income and wealth of the addressee is not entirely new. In fact, Jeremy Bentham proposed the utility-responsiveness of fines as far back as 1789.[154] In many European countries, criminal fines (day fines) already depend on the income of the offender; this is not the case in the UK and the US (except for rare experiments

---

[152] Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEG. STUD. 1 (2009).

[153] *See, e.g.,* Otis H. Stephens, Jr., & John M. Scheb II, 2 American Constitutional Law 480 (14th ed., 2008).

[154] Jeremy Bentham, An Introduction to the Principles of Morals and Legislation, Chapters XII-XV (1789).

with day fines in some communities in the US).[155] Finland has recently introduced income-responsive administrative fines, and Switzerland has enacted income- and wealth-responsive administrative fines, for example for traffic tickets.[156] The rising levels of economic inequality make the debate all the more pressing today. The question of the justification of wealth- or income-responsive fines hinges on the legitimizing reasons for the existence of fines in the first place. If fines are regarded merely as tools to enforce corrective or retributive justice,[157] it may be argued that they should be exactly the same for everybody independent of their social or economic status. However, in recent decades, administrative and criminal sanctions have increasingly been considered to be part of the toolbox of the regulator for steering behavior.[158] This is not to deny that particularly criminal sanctions also have a strong moral and corrective or retributive justice underpinning and that both administrative and criminal fines form part of the expressive function of the law;[159] in fact, our proposal explicitly acknowledges this dimension through the introduction of a "base fine".[160] Nevertheless, the steering component has been identified as one of the key functions of these two types of state action.[161]

If this is true, then the effectiveness of a fine in deterring certain kinds of behavior, such as traffic speeding, will crucially depend on the marginal utility of wealth or income. In economics, the decreasing marginal utility of both wealth and income is almost universally accepted.[162] This implies that a speeding ticket over $50 will be less of a disutility for a millionaire than for a welfare recipient. Therefore, it can be expected to exert less of a behavioral influence on high earnings or on high net wealth individuals than others. Note that both high income and high net wealth reduces the marginal utility of money: this provides a strong reason to correct the amount of fines both for income and for net wealth. This in turn is crucial for an assessment of income- or wealth-dependent fines from the perspective of equality before the law. While it seems clear that greater fines for high income or high net wealth individuals lower economic inequality, they remain contested under a standard of equality that holds that all citizens should be treated alike before the law. However, as was mentioned earlier, the principle of equality not only requires treating sufficiently similar

---

[155] Lance R. Hignite & Mark Kellar, *Day Fines*, *in* THE ENCYCLOPEDIA OF CRIMINOLOGY AND CRIMINAL JUSTICE, published online on January 22, 2014, at 10.1002/9781118517383.wbeccj024; Elena Kantorowicz-Reznichenko, *Day-Fines: Should the Rich Pay More?*, 11 REV. LAW & ECON. 481, 484-85 (2015).

[156] Suzanne Daley, *Speeding in Finland Can Cost a Fortune, if You Already Have One*, NEW YORK TIMES (April 25, 2015), *available at* http://www.nytimes.com/2015/04/26/world/europe/speeding-in-finland-can-cost-a-fortune-if-you-already-have-one.html?_r=0; Christian Demuth, *Raser büßt Tempoverstoß in der Schweiz mit 200.000 Euro*, at http://www.straffrei-mobil.de/ausland/bussgelder/565-raser-buesst-tempoverstoss-in-der-schweiz-mit-200000-euro.

[157] *See, e.g.,* the overview in Gary T. Schwartz, Mixed Theories of Tort Law: Affirming Both Deterrence and Corrective Justice, 75 TEX. L. REV. 1801, 1811-12 (1997).

[158] Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968); *id.*, *Nobel Lecture: The Economic Way of Looking at Behavior*, 101 J. POL. ECON. 385 (1993); STEVEN SHAVELL, FOUNDATIONS OF ECONOMIC ANALYSIS OF LAW 473 (2004).

[159] *Cf.* Cass R. Sunstein, *On the Expressive Function of Law*, 144 U. PA. L. REV. 2021 (1996).

[160] *See infra* note 171and accompanying text.

[161] *See supra*, note 158.

[162] R.D. Collison Black, *Utility*, *in* 8 THE NEW PALGRAVE DICTIONARY OF ECONOMICS 577 (2nd ed., Steven N. Durlauf & Steven E. Blume eds., 2008); HAL R. VARIAN, INTERMEDIATE MICROECONOMICS. A MODERN APPROACH 51-52 (8th ed., 2010). The principle was already used by the 19th century marginalists, see Richard S. Howey, *The Origins of Marginalism*, 4 HISTORY POL. ECON. 281, 283 (1972).

things in the same way, but also treating sufficiently different things differently. If the *raison d'être* of criminal and administrative fines is to steer behavior *ex ante*, it seems persuasive to argue that individual differences in the responsiveness to fines should *require* different amounts of fines in the light of equal protection before the law. The economic responsiveness to fines therefore becomes a crucial distinguishing characteristic that significantly differentiates similar offenses, such as speeding, by different offenders. Income- and wealth-dependent fines therefore foster not only economic but also legal equality.[163]

In fact, income-responsiveness is already a landmark of administrative enforcement against companies when fines are calculated as a fraction of total annual revenue. While antitrust cases have attracted most prominence,[164] it is precisely the field of data protection that is bound to become the new antitrust area in terms of administrative fines. According to the EU General Data Protection Regulation (GDPR) recently voted by the European Parliament, a violation of its provisions can lead to administrative fines in the amount of up to 2% of annual worldwide turnover for undertakings.[165] The original proposal of the European Commission used the language of "proportionate and dissuasive sanctions", a formula, which is preserved in the final version of the Regulation. Thus, from 2018 when the GDPR will enter into force, both national courts and the data protection authorities of the European Member States – their enforcement administrative bodies – will be able to set in place "a system which provides for effective, proportionate and dissuasive penalties."[166] This is a major change after the meager fines levied on Facebook, e.g., for violation of privacy legislation in the past.[167]

We inquire into how Big Data can help in operationalizing the indexing of fines to wealth and income. For example, one of the key problems of adjusting fines to income in the countries in which it is practiced is to determine exactly the relevant amount of income. In Germany, for example, the judge would simply ask the defendant what her monthly income is and perform a plausibility check. However, this often leads to a vast understatement of income by criminal offenders in an effort to lower their fines. Data technologies can be used to automatically, i.e., algorithmically, couple the amount of fines with the earnings and wealth data available to different agencies, for example, to the I.R.S. Simultaneously, robust encryption techniques must be used in order to prevent sensitive data, such as earnings statements of companies or individuals, to become public. The mere transfer of data from the I.R.S. to the administrative or criminal authorities itself does not necessitate the use of Big Data. However, a major problem lies in the validity of the data received by the I.R.S. As is well-known and highlighted by, *inter alia*, the Panama Papers, tax evasion costs the state

[163] *Cf. also* Kantorowicz-Reznichenko, *supra* note 155 (arguing that income-responsive day fines contribute to greater equality of treatment in sanctioning criminal behavior).

[164] See, e.g., John M. Connor, Effectiveness of Antitrust Sanctions on Modern International Cartels, 6 J. IND. COMPET. & TRADE 195 (2006).

[165] Art. 83(4) of the General Data Protection Regulation.

[166] Art. 83(4) read in conjunction to para. 152 of the Preamble, *id*.

[167] *See* PASQUALE, *supra* note 79, at 145. While this type of income-based weighting presents a welcome first step, it chould be coupled with wealth-responsive weighting based on a metric of the total value of the company. This seems even easier to implement than in the case of individual actors: for public companies, the data is freely available in the form of quarterly and annual earnings reports; for nonpublic companies, information from the (Internal Revenue Service) I.R.S. has to be used.

billions of dollars every year, pointing to a significant degree of corruption in the data sets available to tax authorities. Big Data could now potentially be used to provide a better estimate of the real income and wealth of taxed subjects. While the technologies are probably not precise enough at the moment to constitute a firm enough basis to evaluate actual tax calculations on the results, a significant divergence between stated income and/or wealth on the one hand and Big Data driven estimates of real income and/or wealth could trigger heightened scrutiny by the tax authorities. In fact, the Belgian and Dutch tax authorities are already using data mining to single out such "irregular" cases in order to combat tax fraud.[168] Furthermore, some companies such as Kreditech[169] are already leveraging the data mining power of algorithms to calculate the risk profiles of potential lenders.[170] These are used to inform loan decisions. One key parameter for every loan decision is, obviously, the amount of wealth and income of which an individual disposes. The emergence of Big Data lending techniques therefore testifies to the potential of data mining for estimating wealth and income levels.[171] In sum, if the legal and practical difficulties of interagency sharing of information can be overcome, Big Data can help the automatic adjustment of fines to the income and wealth of addressees, something bound to make a major contribution *both* to economic and legal equality.

---

[168] KPMG, *Big data and tax: what is the link?* (2016), available at http://smartalwayswins.kpmg.be/corporate/technology/big-data-and-tax; PWC, *Belgian Minister of Finance Sheds Light on Implementation of BEPS-Related Measures* (December 21, 2015), at 2.

[169] https://www.kreditech.com/what-we-do/.

[170] For a critique of traditional and Big Data credit scoring techniques, such as the FICO score, see Citron & Pasquale, *supra* note 2, at 8-16.

[171] The preceding discussion also provides the key to the practical question about which fines should be responsive to differences in income and wealth. If both essentially serve the same function, i.e., to steer behavior ex ante, both criminal and administrative fines should depend on the level of income and wealth of the perpetrator; in fact, even tort damages should be modified in this way since they equally serve a deterrent function. How can an adjustment of fines to wealth and income levels be technically achieved? Our proposal would be to calculate a weighting factor ϕ for fines, which takes into account both the deviation from average income and average wealth. More specifically, the ϕ factor could represent the arithmetic mean of two ratios: first, the ratio of the income of the offender to average (median) income; second the ratio of the wealth of the offender to average (median) wealth. (The formula for the fine F_o of offender o would then be: $F_o = \phi\ f = [(i_o/i_m) + (w_o/w_m)/2]\ f$, with f representing the base fine, i_o and i_m o's and the median income of the population respectively, and w_o and w_m o's and the median wealth of the population respectively. The use of the median instead of the mean affords the advantage of the median being less affected by very low or high outliers; it is thus less distorted by existing patterns of inequality) The base fine will then be multiplied with the ϕ factor to calculate the adjusted fine for the individual offender. The base fine would be the amount charged today in systems, which do not practice any wealth or income modifications; it thus represents the generic justice dimension of the fine. However, the base fine should constitute a minimum threshold for the weighted fine. Otherwise, agents whose ϕ factor is much smaller than 1 (very poor and/or very low-income people) would be able to engage in sanctioned behavior at close to zero cost, which would not only reduce the deterrence effect in an unacceptable manner but also contradict the retributive justice dimension inherent in the base fine. To sum up, everyone pays at least the base fine; those for whom the ϕ factor is larger than 1 pay a modified, higher fine to account for their greater wealth and/or income.

III. Test Cases

The regulatory tools we highlight serve to both raise awareness for privacy concerns connected to Big Data uses and to mitigate economic and legal inequality in a variety of market settings. The latter objective may be achieved directly (wealth-or income-responsive fines) or indirectly by limiting the amount of data available to companies and by reinforcing the control of users over their data (not only via active choice but also through democratizing data collection and processing, and mobilizing the ex post evaluation of contracts through the unconscionability approach). We test these proposals by hypothetically applying them to three scenarios: social media, student education software, and finally - markets for credit cards and cell phones. The choice of our case studies reflects areas of increased societal concern. In all cases, we show how substantial regulation going beyond transparency can make a difference.

A. Social Media

A first test case that has already surfaced a number of times in the preceding analysis consists in social media services such as Facebook or Google+. While such platforms enable unprecedented forms of communication between diffused and locally remote agents, their creators have also turned them into gigantic data collection engines. The impact of personalization achieved by both companies has been noted both in the sector of personalized advertising and as a political phenomenon such as the so-called "filter bubbles". [172] Moreover, recent studies have shown that Big Data analysis of user behavior on Facebook is strongly predictive of personality traits.[173] In fact, such analysis allows for more fine-grained and more accurate sorting of users into the classical categories of personality psychology (the "Big Five"[174]) than traditional psychological tests do.[175] This is particularly worrisome as such analyses may unlock information that is not only personally but also medically sensitive, and that may be used to discriminate against certain psychological types. Thus, while Big Data can have negative externalities for consumers more generally, such negative externalities multiply for vulnerable groups that might or, in certain case, might not be even users of social media networks. Cyber bulling is despicable for all of its victims, but for example revenge

[172] *See, e.g.*, Frederik J. Zuiderveen Borgesius, Damian Trilling, Judith Moeller, Balázs Bodó, Claes H. de Vreese & Natali Helberger, *Should We Worry About Filter Bubbles?*, 5 (1) INTERNET POL'Y REV 1 (2016). Filter bubbles refer to the phenomenon of users being confronted mainly with opinions and content which matches their pre-existing views, thus driving out dissent and variety in opinion formation.

[173] Jacopo Staiano, Bruno Lepri, Nadav Aharony, Fabio Pianesi, Nicu Sebe, and Alex Pentland, *Friends don't Lie – Inferring Personality Traits from Social Network Structure*, Proceedings of the 2012 ACM Conference on Ubiquitous Computing – UbiComp '12 (2012), Sept. 5-8, 2013, Pittsburgh, PA, USA, ACM, http://dx.doi.org/10.1145/2370216.2370266; Mitja D. Back, Juliane M. Stopfer, Simine Vazire, Sam Gaddis, Stefan C. Schmukle, Boris Egloff & Samuel D. Gosling, *Facebook Profiles Reflect Actual Personality, Not Self-Idealization*, 21 PSYCH. SCI. 372 (2010).

[174] The *locus classicus* is Ernest C. Tupes & Raymond E. Christal, *Recurrent Personality Factors Based on Trait Ratings* (USAF Tech. Rep. ASD-TR-61-97), Personnel Laboratory, Lackland Air Force Base, TX, 1961; good overview in Robert R. McCrae & Oliverd P. John, *An introduction to the five-factor model and its applications*, 60 J. PERS. 175 (1992). The five personality traits are openness, conscientiousness, extraversion, agreeableness, and neuroticism.

[175] See Staiano, Lepri, Aharony, Pianesi, Sebe & Pentland, *supra* note 173.

pornography can have especially dire consequences for the employment and other basic life opportunities of those affected (overwhelmingly women).[176]

The regulatory strategies we propose can be expected to at least mitigate these risks. Mandating active choice between a data-free and a data-collection option can be economically viable if an inverse predatory pricing oversight of the data-free option is introduced.[177] As has furthermore been noted, enabling a maximally informed choice on the options is crucial. Therefore, when it comes to social media, the notice should not only point to the value of personal data disclosed in the data-collection alternative but also remind users of the far-reaching consequences that access to their data can have. A full notice prompting active choice for Facebook users may therefore be designed as follows:

Your Choice! ***You may now choose between two different options to sign up for Facebook:***	
Data Collection Option	**Data Free Option**
For this option, **you pay with your data**. An average user gives away **monthly data worth about $4**.	For this option, **you pay with your money** instead of your data. The **monthly price is $[x]**.
The collected data **enables** the construction **of your entire psychological profile**. Each time you log on, imagine you start a new session with a company psychiatrist.	This option does **not allow** for the construction of a **psychological profile**.

The reasonableness requirement for the price of the data-free option, which we advocate would impose a dual constraint. First, the price must remain within 1.5 times the average variable cost of the provision of service. Second, it may not exceed the marginal value of personalized data. While we lack data for average variable cost at the moment, the latter constraint imposes a limit of $6 for the monthly price of the data-free option of Facebook. It seems that such a reasonable price might motivate a significant number of privacy-minded users to switch to a data-free option. To the very least, pricing is prevented from becoming prohibitive by the reasonableness control we propose.

As long as the active choice regime is not yet installed by legislation, courts may resort to the doctrine of unconscionability to strike down specific privacy provisions in EULAs or similar contracts. As was noted, the current take-it-or-leave-it nature of privacy policies creates a

[176] *See, e.g.*, Danielle K. Citron & Mary A. Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. (2014). Whereas in recent years the anti-revenge porn movement has achieved significant results in enacting statutes that criminzalize this practice in the states, a federal bill is still missing. Our policy proposals therefore remain relevant.

[177] *Supra*, Part II.B.1.

significant imbalance in bargaining power and deprives users of meaningful choice. At least under the California doctrine, the procedural prong of unconscionability is therefore fulfilled. However, provisions also need to be substantially unconscionable to be struck down under the unconscionability test.

On a general level, it may be argued that one potential source of substantial unconscionability resides in the very framework of the data policies of social media providers such as Facebook: the fact that by using personal user data massive amounts of profits are generated without sharing any of these profits with the users. Obviously, users gain nonmonetary advantages from using Facebook and other social media networks. However, if these user benefits are dwarfed by the company benefits, the doctrine concerning grossly inadequate pricing (substantive unconscionability) could be mobilized.[178] The cases coming down under this prong of the test have traditionally compared a market price with the actual price charged. The problem in data-collecting services is that a monetized market price for comparable services does not exist, leaving the courts without a yardstick to determine whether the value of data disclosed is inadequate vis-à-vis the services offered. Nonetheless, the fact that all revenue from the data unilaterally goes to the social media provider could motivate a finding of unfair one-sidedness of the contract. As we have seen, however, the marginal revenue generated from personalized data of a single user amounts to approximately $1-10 per month in the case of Facebook. This does not seem to make the contract "so one-sided as to shock the conscience."[179]

In any event, specific features of the data policies may qualify for substantial unconscionability. For example, Facebook states in its data policy that "we use the information we have to improve our advertising and measurement systems so we can show you relevant ads on *and off* our Services." [italics added by the authors] "We work with third party companies […] who use advertising or related products […]." "We transfer information to vendors, service providers, and other partners who globally support our business […]."[180] According to industry sources, the personalization of non-Facebook websites by means of Facebook data is a growing source of revenue for Facebook that will likely be expanded in the future. Such selling of collected data to third parties may be deemed "unreasonably favorable" to Facebook.[181] While it may still seem conscionable that Facebook uses user data to generate revenue via advertising on its own website, this evaluation changes when data are sold to third parties. First, users generally expect data to be used for advertising on Facebook; this may be less true for third-party websites.[182] Second, this policy strikes down all barriers that would contain personal information within the (already vast) domain of Facebook. Rather, personal

[178] *See, e.g.*, Kugler v. Romain, 58 N.J. 522 (1971); Jones v. Star Credit Corp., 298 N.Y.S.2d 264 (Sup. Ct. 1969); Fleet v. United States Consumer Council, Inc., 22 Ill.95 B.R. 319 (E.D. Pa. 1989); *see also* Kornhauser, *supra* note 135, at 1159-61.

[179] Kinney v. United Healthcare Servs., Inc., 83 Cal.Rptr.2d 348, 353 (Ct.App.1999); Ferguson v. Countrywide Credit Industries, Inc., 298 F.3d 778 (9th Circ. 2002).

[180] Facebook, Inc., Data Policy, https://www.facebook.com/policy.php.

[181] *See* for this standard Williams v. Walker-Thomas Furniture, 121 U.S. App. D.C. 315 (1965).

[182] *But see* Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 600 (2014) (showing that a majority of respondents in a randomized survey did expect Facebook to share data with third parties).

data are spread around the web, creating unforeseeable risks of data leaks and loss of control for users while unilaterally benefiting Facebook in the generation of revenue. This causes a profound imbalance of contractual duties so that a verdict of substantial unconscionability would be well motivated.

Our third proposal extends to the democratization of data collection. We suggest that large companies like Google or Facebook would have to regularly conduct surveys among their current as well as potential new users (who might be put off by their data policies but nevertheless generally interested in using their services). The survey would generate representative data on the feelings and preferences of participants toward the data policies of the social media providers. The results would need to be disclosed publicly. As Ian Ayres and Alan Schwartz have implicitly argued in a related context, requiring large companies to regularly conduct surveys does not amount to an excessive burdening of the providers.[183] Furthermore, privacy protection would certainly benefit from an institutionalized data protection compliance officer democratically elected by users.

Finally, it is particularly relevant to change to a regime of revenue- and wealth-responsive fines for the violation of data privacy rules when dealing with highly capitalized companies such as Facebook or Google. Any system of fixed rate fines will most likely not produce any tangible deterrent effect, as can be noted in the controversial behavior of the company so far. The provision in the EU General Data Protection Regulation mandating fines up to 2% of global annual turnover is a step in the right direction.[184] The widespread use of social networks and search engines makes our proposal impactful for consumers generally. As our hypothetical case study has shown, implementation of our policy proposals will give users the opportunity for making real choices about their data when they use such services. More importantly however, our first case study has shown the real-life impact that active choice, unconscionability, the democratization of data collection and wealth-responsive penalties can have for groups that can easily suffer discrimination caused by Big Data.

B. Student Education Software

Over the past decade, the introduction of new software for individualized learning across schools in the US has generated numerous opportunities for improving the education process, while also triggering a number of legitimate concerns[185] over the use of student data for marketing or other purposes than what the information was originally collected for (e.g. for compiling student profiles that can later be sold to data brokers, future employers etc.). Since current federal legislation[186] offers limited protection only, bipartisan legislative drafts

[183] Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 584 (2014) (noting that "[t]he seller must establish through independent testing that a majority of consumers who read the box learn the true impact of the unexpected term.").

[184] Art. 79(6) of the General Data Protection Regulation.

[185] Joel Reidenberg, N. Cameron, Jordon Kovnot, Thomas B. Norton, Ryan Cloutier, and Daniela Alvarado, Privacy and Cloud Computing in Public Schools, Center on Law and Information Policy (2013).

[186] Family Educational Rights and Privacy Act (FERPA), Pub. L. No. 93-380 (1974), codified at 20 U.S.C. § 1232g. FERPA covers only educational agencies or institutions that receive funds through particular programs administered by the United States Secretary of Education. Even if covered by FRPA, schools that have contracts with cloud computing service providers may be able to circumvent the statute's provision for parental consent

have been introduced to close some of the flagrant loopholes.[187] In the meantime, attempts to regulate the field have also emerged in various states.[188]

Not all of our proposed strategies can be applied to this sector. A data free-option might imply more expenses for poor parents on the one hand, and jeopardize the efficient roll-out of personalized learning for all, on the other. However, implementing some of the suggestions we have made in this article to the area of student privacy will supplement the tabled legislative proposals in various ways. First, as with the test case on social media, the substantial prong of the unconscionability doctrine can be evoked if student records are shared with third parties without parental control, and solely for the enrichment of software providers. In order to avoid being held responsible under the procedural prong (take-it-or-leave-it offers) and still modernize the learning process, school boards might want to have parents participate and vote in the selection of student learning software providers. This will ensure that children's interests are represented in a more robust manner and will arguably increase the bargaining power of the school in negotiating not only competitive prices but also non-discriminatory storage and use of educational records. A troubling issue with the existing federal legislation is that it does not give students or parents meaningful control over students' personally identifiable information (PII) collected by the software providers. Further democratizing the process by requiring the software providers to conduct surveys would allow for systemic monitoring of the parents' and students' actual preferences. Ultimately, subjecting the contracts that schools enter into with software education providers to ex post evaluation in the light of the unconscionability doctrine would ensure that there are no irregularities.

Finally, one of the prominent criticisms of the existing federal statute is that it does not impose strong penalties. Applying a wealth-responsive fine to companies that sell student data or use it for targeted advertising will deter them from such violations in the future without unnecessarily burdening the start-ups that are experimenting with the development of new learning personalization software solutions. Similarly, a wealth-responsive fine can constitute a proportionate response to the concerns of some education software providers who are unhappy with the lack of a level playing field, given that under some of the tabled proposals fines might apply to private companies but not to the non-profit sector or the school districts that might also breach student privacy.[189]

---

under the statutory exception for "school officials", broadly interpreted under FRPA. *See* e.g. Dalia Topelson Ritvo, Privacy and Student Data: An Overview of Federal Laws Impacting Student Information Collected Through Networked Technologies, The Berkman Center for Internet & Society at Harvard University (2016).

[187] For a comparison of relevant provisions of the Californian Bill (SOPIPA) with the proposed in 2015 Polis-Messer Federal Bill and a voluntary code of conduct, see Brenda Leong, Future of Privacy Forum, https://fpf.org/wp-content/uploads/FPF-DeID-FINAL-7242015jp.pdf.

[188] For variations of student privacy regulations that either require K-12 schools to contractually oblige vendors to safeguard student privacy and security, prohibit secondary uses of student data without parental consent or introduce measures for the collection and use of pupil data, *see* NATIONAL CONFERENCE OF STATE LEGISLATURES, at http://www.ncsl.org/research/education/student-data-privacy.aspx.

[189] *See Supra* note 102, Petkova.

C. Credit Card and Cell Phone Markets

Another example concerns more traditional markets on which customer data are collected on a large scale, often to the detriment of customers: credit card and cell phone markets. As Oren Bar-Gill and others have shown in a range of impressive studies, providers use the data collected to design contracts that exploit the weaknesses of consumers.[190] These are clear cases of what Ryan Calo has called "digital market manipulation";[191] in the economics literature, these are also dubbed "exploitative contracts".[192] A particularly telling example is the study by Shui and Ausubel based on a data set they obtained from a large commercial US bank.[193] The bank sent offers containing different credit card contracts to 600,000 US customers. The most popular tariff unsurprisingly turned out to contain a teaser rate with a low introductory and a high back-end interest rate.[194] The bank monitored the spending behavior of those recently acquired credit card customers over a longer time. The data revealed that 79% of customers who had chosen the teaser rate had opted for the wrong contract – assuming equal spending behavior, a non-teaser contract would have served them better.[195] If – as can be assumed – the bank uses these data to specifically offer the teaser rates to these consumers, this is a classical example of adverse targeting.[196] As Duncan McDonald, former general counsel of Citigroup's Europe and North America credit card section, puts it:

> "No other industry in the world knows consumers and their transaction behavior better than the bank card industry. It has turned the analysis of consumers into a science rivaling the studies of DNA. The mathematics of virtually everything consumers do is stored, updated, categorized, churned, scored, tested, valued, and compared from every possible angle in hundreds of the most powerful computers and by among the most creative minds anywhere. In the past 10 years alone, the transactions of 200 million Americans have been reviewed in trillions of different ways to minimize bank card risks."[197]

Notably for our context, credit markets do not only offer potential for exploitation, however, but also for discrimination. Studies suggest that racial discrimination is still prevalent in the credit sector, with African-American and Hispanic citizens' access to credit

---

[190] BAR-GILL, *supra* note 17, Chapters 3 and 4, particularly at 217-223; Michael D. Grubb, *Selling to Overconfident Consumers*, 99 AM. ECON. REV. 1770 (2009).

[191] Calo, *supra* note 7.

[192] Paul Heidhues & Botond Kőszegi, *Exploiting Naïvete about Self-Control in the Credit Market*, 100 AM. ECON. REV. 2279 (2010); Paul Heidhues, Botond Koszegi & Takeshi Murooka, *Inferior Products and Profitable Deception*, Working Paper (2012), *available at* https://www.esmt.org/inferior-products-and-profitable-deception; Botond Kőszegi, *Behavioral Contract Theory*, 52 J. ECON. LITERATURE 1075, 1104-10 (2014).

[193] Haiyan Shui & Lawrence M. Ausubel, *Time Inconsistency in the Credit Card Market*, unpublished manuscript (2005), *available at* http://web.natur.cuni.cz/~houdek3/papers/economics_psychology/Shui%20Ausubel%202006.pdf.

[194] Shui & Ausubel, *supra* note 193, at 8-9.

[195] Shui & Ausubel, *supra* note 193, at 9.

[196] *See supra* note 8.

[197] Duncan McDonald, *Viewpoint: Card Industry Questions Congress Needs to Ask*, AMERICAN BANKER (March 23, 2007), *available at* http://www.americanbanker.com/issues/172_58/-306775-1.html; *see also* Charles Duhigg, *What Does Your Credit-Card Company Know about You?*, NEW YORK TIMES (May 12, 2009), available at http://www.nytimes.com/2009/05/17/magazine/17credit-t.html?_r=0.

being significantly restricted.[198] Protected groups, moreover, more generally continue to face discrimination in consumer markets, being offered worse conditions, higher prices, and less service.[199]

How would the regulation we propose change the picture? First of all, the mandated active choice regime would raise awareness of the amount of data collection in the credit card business of which many consumers are currently unaware. Furthermore, it would enable a real choice between a tariff with higher interest rates but no data collection and one with the inverse features. Particularly vulnerable groups may use this option to prevent explicit or implicit instances of discrimination by algorithms. Second, unconscionability could be mobilized in order to invalidate provisions in credit card contracts allowing the selling of data to third parties. A major issue in this context would be whether the verdict of unconscionability would also extend to the transmission of data to credit-scoring companies. At least theoretically, it may be claimed that credit-scoring companies provide useful services in the marketplace and that they enable risk allocation in different contracts. However, given the opaque nature of scoring combined with its potentially far-reaching consequences for the scored subjects,[200] it may be reasonably argued that scoring agencies present a significant and hard to determine risk for the affected party. This may motivate a finding of such a provision to be unreasonably one-sided. Third, the moves discussed under the header of democratization would require large companies to conduct surveys on the willingness of subjects to be scored. Furthermore, they would need to obtain explicit consent in order to change their privacy provisions toward more data collection, sharing and processing. The greatest contribution, however, may come from the institutionalization of a data privacy compliance officer. She could monitor the ways and purposes of data collection and blow the whistle if the data collected is used in exploitative contracts to the detriment of customers. The compliance officer would therefore regularly report to a supervisory authority such as the FTC or the CFPB whenever practices such as those uncovered by Shui and Ausubel[201] or Bar-Gill[202] are prevalent in the company.

Finally, fines which sanction violations of privacy regulation and administrative or criminal proceedings would have to be adapted to the revenue and value of the company in order to achieve effective deterrence. In the case of exploitative contracts, they could be coupled with the disgorgement of profits either to the exploited parties or to the supervisory authority.

IV. Conclusion

This article spells out the hitherto unrecognized ambivalence of Big Data regarding its tremendous potential to entrench existing inequalities but also to promote an equality agenda in new and powerful ways. Recent scholarship has stressed Big Data's potential to create both intentional and unintentional discrimination. We pick up on this problematic aspect, and

[198] Pager & Shepherd, supra note 36, at 189-91.
[199] Pager & Shepherd, supra note 36, at 191-92.
[200] PASQUALE, *supra* note 79, Chapters 2 and 4; Citron & Pasquale, *supra* note 2, at 8-16.
[201] *See supra* note 193.
[202] BAR-GILL, *supra* note 17, Chapters 3 and 4, particularly at 217-223.

expand and complicate it by unfolding the potential of Big Data to reduce both legal and economic inequality. Big Data's ambivalence hinges on its unique quality to differentiate between different situations and persons – for good or for bad. The key challenge for the law is to facilitate useful distinctions between differently situated agents while curbing illegitimate discrimination.

We review a range of regulatory tools, which are novel in this context and can help in achieving the ambitious task of reining in Big Data's potential. As a corollary, some of these approaches promote transparency, a desideratum highlighted in much of the previous scholarship. The new regulatory models we suggest contribute to a prevention of the exploitation of all users by asymmetrically better-situated market players but are even more relevant for groups vulnerable to discrimination. The use of algorithmic decision-making creates unfortunate economic incentives for new forms of discrimination that do not easily square with the current anti-discrimination doctrine. Four regulatory instruments stand out: First, active choice may be mandated between data-collecting and data-free services, coupled with a novel form of price control derived from antitrust law. The latter feature ensures that a data-free option is not merely hypothetical but is an economically realistic option. Second, as long as such strategies are not enacted by law, we propose using the doctrine of unconscionability to institutionalize the ex post review of contract clauses which unreasonably favor the data-collecting or processing company. Third, data collection and processing should be democratized. This can be achieved primarily through mandatory surveys of current and potential users on the one hand, and through the institutionalization of a high-level data protection compliance officer, to be elected by current users, on the other. Finally, we note that income- (or revenue-) and wealth-responsive fines, both for individual persons and for companies, provide a unique tool to couple effective and just deterrence with the reduction of both economic and legal inequality.

This array of tools must be adapted to different contexts and situations. We review three cases in which they may bring new solutions to old problems. In the context of social media, all four instruments can counter the increasing loss of control of users over their own data. Education software can make use of some of the outlined solutions. In the realm of credit card and cell phone contracts, where adverse targeting and exploitative contracts have been both empirically and theoretically found to be rampant, our approach may substantially curb the power of providers to unilaterally use data to the detriment of their clients.

Many more examples could and should be discussed. In the face of increasing unease about the asymmetry of power between Big Data collectors and dispersed users, about differential legal treatment, and about the unprecedented dimensions of economic inequality, this article proposes a new regulatory framework and research agenda to put the powerful engine of Big Data to the benefit of the individual.