Public Comments Submitted for:
The Federal Trade Commission
Big Data: A Tool for Inclusion or Exclusion? Workshop, Project No. P145406

Submitted by:
Dennis D. Hirsch
Geraldine W. Howell Professor of Law
Capital University Law School

Big Data can create tremendous social and economic value. But it can also cause harm. For example, companies could use data analytics to identify which people are most likely to get sick, get pregnant or go bankrupt, and then deny employment, loans or insurance to these individuals even where the condition (illness, pregnancy, bankruptcy) has not yet occurred. Privacy regulators and privacy professionals will be asked to respond to these uses of Big Data.

They will not be able to employ traditional privacy regulation to do so. The dominant privacy law framework, which is premised on notice, choice and purpose limitation, is ill-equipped to deal with Big Data. The reasons for this are straightforward. Notice of intended collection is impractical in a world of ubiquitous data collection. Notice of intended uses is all but impossible where data analysts do not know in advance how they will use the data. Without effective notice, individuals cannot make meaningful choices. Finally, data analytics requires continual re-purposing of data and so is antithetical to purpose limitation. The existing privacy law paradigm is a poor fit for Big Data. Another approach is needed.

What should this new approach be? To find an answer, it helps first to explore a bit more how it is that Big Data and data analytics can cause harm. Once we have defined the threats, we are on our way to finding a solution to them. As will be explained below, I believe that the answer may lie in FTC's Section 5 "unfairness" jurisdiction, and that the New Jersey District Court's recent decision *FTC v. Wyndham Worldwide Corp.*, No. 13-1887 (D.N.J. April 7, 2014), shows how the FTC can use this authority to provide the needed protection.

How can Big Data hurt people? Assume a de-identified database of individuals, some of whom have diabetes. The database contains many data points about these individuals gleaned from their Web travels, supermarket purchases, public records, and other common sources of personal information. Data analysts search for common factors – correlations – that link those who have diabetes and distinguish them from those who do not. This yields a "profile" of diabetes sufferers – a set of characteristics that they share, other than the disease itself. Analysts can then apply this profile to the general population in order to identify others who have diabetes or are likely to suffer from it in the future.

Society can benefit greatly from such an insight. For example, policymakers or health care providers might use it to target preventative care to those deemed likely to suffer from diabetes in the future, thereby improving and even saving lives. But the profile can also be used in other, less wholesome ways. As alluded to above, companies might use the same profile to predict who is likely to get diabetes and, on this basis, deny these individuals job interviews, loans, apartment rentals or insurance. While these actions may benefit the business, they offend basic societal notions of equal opportunity and free will (after all, some of these individuals may have taken preventative measures themselves and avoided the disease). If the profile correlates to a particular race, religion, gender or other protected class, this practice may also violate non-discrimination values and laws.

At their core, these injuries are not about notice, consent, or control of personal information. They are about fairness – about whether it is fair for companies to use predictive profiles in this way. Protecting individuals against these harms will require us, as a society, to figure out which uses are appropriate and beneficial (e.g. preventative care for likely diabetics), and which are damaging and unfair (e.g. denying jobs, loans or apartments to these individuals). The traditional "notice and choice" model of privacy regulation does not provide a way to sort this out.

FTC's unfairness jurisdiction does. Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices" that affect commerce. To date, the Commission has largely focused its enforcement efforts on "deceptive" corporate behavior – an enforcement strategy that is linked to, and supports, the notice and choice approach to privacy regulation. When it comes to addressing Big Data's threats, the FTC may find that its unfairness jurisdiction proves even more useful.

Section 45(n) of the FTC Act provides that the FTC can declare an act or practice to be unfair if it: (1) "causes substantial injury to consumers;" (2) the injury "is not reasonably avoidable by consumers themselves"; and (3) the injury is "not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). Section 45(n) further provides that, in determining whether a given act or practice is unfair, the "Commission may consider established public policies as evidence to be considered with all other evidence," although "[s]uch public policy considerations may not serve as a primary basis for such determination." *Id.*

This legal framework fits nicely with the issues that Big Data presents. As to the first factor, denial of employment, a loan or a similar benefit or opportunity can constitute a substantial harm. As to second, most consumers will not understand data analytics, predictive profiles, and how these growing practices will affect them. They cannot "reasonably avoid[]" the harm through their own actions in the marketplace. The third component – whether these harms outweigh "countervailing benefits to consumers or to competition" -- is exactly what society needs to sort out. It needs to identify core values (opportunity, free will, equality) and weigh them against the efficiencies and social benefits that Big Data can provide. The third prong provides a vehicle through which FTC can undertake this crucial balancing.

The FTC Act even gives the Commission guidance on how to go about determining whether a given secondary use – e.g. using diabetes predictions to deny employment or loans – is, or is not, "unfair." The Act states that, in making these calls, the Commission "may consider established public policies as evidence" of unfairness. Thus, FTC should be able to consider, and weigh against Big Data's benefits, the values contained in such established laws and policies as: constitutional doctrines of equal protection and due process; anti-discrimination laws; rules governing racial profiling; statutes, such as the Genetic Information Non-discrimination Act, that limit secondary uses of personal data; state laws limiting employer access to and use of employee social media postings; and FTC's own established policies regarding unfair business practices. In a future article, I will analyze these "established public policies" and explore what they tell us about how to distinguish fair and appropriate uses from unfair and inappropriate ones.

For now, it is important to say a few words about whether the FTC actually has the power to use its unfairness authority in the way that I have proposed. That is where the New Jersey District Court's recent decision in the Wyndham Hotels case comes in. While FTC has rarely used its unfairness authority to enforce against privacy-related injuries, it has used it more regularly to enforce against companies that unreasonably fail to secure individuals' personal data. In *Wyndham*, FTC alleged that the hotel chain had experienced not one but three, similar security breaches without taking appropriate steps to prevent them. FTC claimed that this was unfair to the hotel chain's customers who depended on the company to safeguard their data.

The company refused to settle and, instead, challenged FTC's authority to bring the unfairness claim. The *Wyndham* case thus tests the scope of FTC's unfairness authority in the digital age. The FTC passed the test. The District Court denied the company's motion to dismiss and upheld the Commission's interpretation of its unfairness authority. Assuming that that court of appeals upholds it, the *Wyndham* decision should considerably strengthen FTC's ability to use its unfairness jurisdiction. While the *Wyndham* decision concerns corporate security practices, its logic may well extend to enforcement against unfair profiling practices.

The *Wyndham* decision is also important in another way. The hotel chain argued that, if FTC is going to apply its unfairness authority in this way, it must do so through general rules promulgated in advance. FTC argued for a more case-by-case, incremental approach to policymaking. Once again, the District Court agreed with the Commission's position. For the present purposes, this means that FTC could, potentially, use case-by-case adjudicative processes to build series of decisions about which uses of predictive profiles are fair, and which are not.

Such an approach has its negative and positive sides. On the one hand, it lacks certainty. On the other, it provides regulators with the flexibility to treat each situation on its merits. It also gives the Commission space to feel its way forward in this rapidly changing field before developing hard and fast rules on what is fair, and what is not. Most importantly, an evolving set of FTC enforcement actions could provide a way to sort out the benefits and harms of Big Data profiling, and to balance them. That is a task that society must undertake if it is to unlock Big Data's great potential, without creating a fairness-based backlash.