Federal Trade Commission

Big Data: Shining a Light into the Black Box

Jessica Rich[1]
Director, Bureau of Consumer Protection, FTC

Public Citizen
May 11, 2015

Thank you. I'm delighted to be here today to discuss the important topic of Big Data and its effects on consumers. And I'm especially pleased to be sharing this panel with Frank Pasquale and Peggy Twohig, my longtime colleague and friend from our years together at the FTC and now an important partner at the CFPB.

"Big Data" is a term we're hearing a lot lately and it can mean many different things, depending on who's using it and the context. It's become such an integral part of our current lexicon that it's even the name of a popular alternative Rock Band, which has a current hit called (perhaps aptly) "Dangerous."

When most of us in this room refer to "Big Data," we're generally talking about the confluence of three factors, which together have a profound effect on consumers.

[1] The views expressed here are my own and do not necessarily represent the views of the Federal Trade Commission or any Commissioner. Special thanks to Molly Crawford for assisting in the preparation of these remarks.

First is the ubiquitous collection of consumer data through the Internet, social media, mobile devices, and sensors. Think Google and Facebook, your mobile phone, your fitness tracker, your new Smart Car, retail tracking. It's everywhere. Second is the plummeting cost of storing data, which has enabled and encouraged ever more collection and use of this data, much of it sensitive. And third is the powerful new capability to analyze data to draw connections and make inferences and predictions.

In other words, we're talking about the "three Vs" – volume, velocity, and variety of data – each of which is proliferating at a rapid rate, and which together allow for the analysis and use of data in ways that weren't previously possible.

As we know, Big Data is now increasingly being used to make decisions about a wide range of issues affecting consumers. The FTC held a workshop on this issue last fall, entitled *Big Data, A Tool for Inclusion or Exclusion?*, to discuss both the consumer benefits and potential harms of this phenomenon, focusing in particular on low-income and underserved consumers.[2] Certainly, there are benefits. For example, Big Data is being used to develop alternative credit scores for consumers who don't have traditional credit histories and were previously considered "unscorable" and thus ineligible for credit. Big Data also can increase access to education – for example, by identifying students for advanced classes who otherwise would not have been chosen based on the usual criteria or, alternatively, students at risk of dropping out and in need of help.

---

2 *See* FTC Workshop, *Big Data: A Tool for Inclusion or Exclusion?* (Sept. 15, 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion.

Big Data also offers health and safety benefits. For example, it can be used to predict life expectancy, genetic predisposition to disease, and likelihood of hospital readmission –allowing health care providers to develop more effective treatment plans and lower health care costs. Or, as the Washington Post article on this topic mentioned yesterday, it could be used to find cancer clusters or contaminated waterways.[3]

But each of these benefits has a flip side: just as Big Data can be used to extend credit, educational opportunity, and health benefits to consumers, so too can it be used to deny those services. For example, there are now scores for everything, from consumer profitability scores, which predict households that are likely to be profitable and pay debts, to fraud scores that predict whether a consumer is masquerading as another or engaging in other mischief. These scores can be used to deny consumers the ability to complete transactions, without any explanation. Further, if online companies charge consumers in different zip codes different prices, one result could be that consumers in poorer neighborhoods pay more for online products than consumers in affluent communities. And in the FTC's fraud program, we are seeing consumers targeted again and again by scam artists, using detailed consumer data bought from other companies that includes bank account numbers, Social Security numbers, and lending histories.

With the growing popularity of wearable health devices, the effects of Big Data may be particularly dramatic when it comes to the collection and use of consumers' sensitive health data. According to yesterday's Washington Post article, surveys show

3 Ariana Eunjung Cha, *The Human Upgrade*, Wash. Post, May 9, 2015, *available at*

that an estimated 68 million wearable devices will be shipped this year, and that many consumers share information collected through these devices with someone else.[4]

These are the challenges that consumers face today, and they are considerable. But the FTC has an active program to address them.

First, we are doing what we can to open the Black Box and shine a light on Big Data practices. For example, last year we released a report on our in-depth study of nine data brokers representing a cross-section of the industry.[5] The report discussed how data brokers acquire and store billions of data elements on nearly every U.S. consumer and develop detailed profiles for sale to other companies. It also discussed how data brokers don't just collect and share raw data, but also develop inferences about people and put them into categories – such as Urban Scramble and Mobile Mixers, which characterize low-income, minority consumers; Thrifty Elders; and Financially Challenged. Virtually all of this happens behind the scenes, without consumers having any idea, let alone control over it. The report called on Congress to pass legislation requiring greater transparency, including by giving consumers access to their data and choices about how it will be used. Notably, the report also called on consumer-facing entities, such as retailers, to provide choices to consumers before sharing data with data brokers.

Also, as I mentioned, the FTC held its Big Data workshop last fall to examine the other side of the transaction – whether and how the use of Big Data is benefiting

---

http://www.washingtonpost.com/sf/national/2015/05/09/the-revolution-will-be-digitized/.

4 *Id.*

consumers or excluding them from full opportunity in the marketplace.[6] We intend to release a report on the workshop later this year.

Second, the FTC is enforcing the laws currently on the books that address uses of Big Data that harm consumers. One of the big messages we want to send to businesses and the public is that there are indeed laws that apply here, and they must be followed. These laws include the Fair Credit Reporting Act (FCRA),[7] the Equal Credit Opportunity Act (ECOA),[8] and the FTC Act's ban on unfair and deceptive practices.[9]

The FCRA is a particularly valuable tool in this area because it contains requirements for ensuring the accuracy and privacy of data used to make credit, employment, insurance, and other important decisions about consumers. Enforcing this law has been and continues to be an FTC priority. To date, we've brought 100 FCRA cases and obtained over $30 million in civil penalties. And we are increasingly bringing cases against non-traditional consumer reporting agencies – often, data brokers that sell data for FCRA-covered activities without complying.

For example, we recently entered into consent decrees with InfoTrack[10] and Instant Checkmate,[11] data brokers that sell detailed background checks to employers and

---

5 FTC Report, *Data Brokers: A Call for Transparency and Accountability* (May 2014), *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
6 *Supra* n.1.
7 15 U.S.C. §§ 1681–1681x (2012).
8 15 U.S.C. § 1691(a).
9 *See* 15 U.S.C. § 45(a)(1).
10 *U.S. v. Infotrack Information Servs., Inc. et al.*, No. 1:14-cv-02054 (N.D. Ill. Mar. 24, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3092/infotrack-information-services-inc-et-al.
11 *U.S. v. Instant Checkmate, Inc.*, No. 3:14-cv-00675-H-JMA (C.D. Cal. Apr. 9, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3221/instant-checkmate-inc.

landlords for use in deciding whether to provide consumers with jobs and housing. Our complaints alleged that these companies failed to ensure the data was accurate, or that the purchasers had a permissible purpose to buy it, as required by the FCRA. The orders included civil penalty judgments of $1 million for InfoTrack and $525,000 for Instant Checkmate.

Similarly, our cases against Telecheck[12] and Certegy[13] involved data brokers that sold consumer data to companies deciding whether to accept checks from consumers in stores. As you know, consumers that write checks in stores are often elderly, illustrating the importance of the FCRA for protecting certain consumer groups. The companies each paid $3.5 million in civil penalties.

Even companies that are well-versed about the FCRA and purport to comply need watching. A few years ago, we brought a case alleging that Equifax sold prescreened lists of consumers who were late on their mortgage payments – which were consumer reports – to another company that then sold this information to companies that used it to pitch fraudulent debt relief services to consumers in financial distress.[14] Similarly, we took action against TeleTrack, a consumer reporting agency serving the subprime marketplace, for selling its consumer report information to marketers – including lists of

12 *U.S. v. Telecheck Servs., Inc.*, No. 1:14-cv-00062 (D.D.C. Jan. 16, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3183/telecheck-services-inc.
13 *U.S. v. Certegy Check Servs., Inc.*, No. 1:13-cv-01247 (D.D.C. Aug. 15, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3184/certegy-check-services-inc.
14 *Equifax Information Servs.*, Docket No. C-4387 (Mar. 5, 2013) (F.T.C. order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3252/equifax-information-services-ll.

consumers who had applied for payday loans.[15] We now know that these types of lists are a big source of the phantom debt fraud we are seeing throughout the marketplace.

The FCRA also covers those who purchase and use consumer report information. If a company buys this information from a CRA and uses it to make decisions about consumers' employment, credit, insurance, or housing, and certain other benefits, the FCRA applies. This means that, among other things, companies must provide consumers with adverse action notices if they decide to deny these benefits to consumers. Similarly, companies also must now provide risk based pricing notices if they use consumer reports to provide credit to consumers on less favorable terms than other consumers. For example, we brought an action against Time Warner Cable, and obtained almost $2 million in civil penalties, because the company used consumer reports to decide whether to require consumers to pay a deposit on their cable bills, but failed to provide these consumers with risk-based pricing notices.[16]

In addition to the FCRA, there is also the ECOA and the FTC Act. The ECOA prohibits discrimination in credit based on protected characteristics such as race, color, gender, and age. So, if a company makes credit decisions about individuals based on Big Data, it could violate the ECOA if the decision leads to disparate treatment or disparate impact on those individuals. There's a lot more to the analysis, to be sure, but I wanted to highlight the applicability of this important law to the Black Box.

---

15 *U.S. v. Teletrack, Inc.*, No. 111-CV-2060 (N.D. Ga. June 27, 2011), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3075/teletrack-inc.
16 *U.S. v. Time Warner Cable, Inc.*, No. 13-cv-8998 (S.D.N.Y. Dec. 19, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3149/time-warner-cable-inc.

And, of course, the FTC Act is a highly valuable law here – it prohibits unfair or deceptive practices across most of commerce, and the FTC has used it in many contexts to protect consumers at financial risk. One key area of concern is the increasing ability of scam artists to purchase detailed information about consumers and use it to perpetrate fraud. For example, as I mentioned, we've seen many so-called phantom debt scams in recent years, in which companies contact consumers who may have applied for payday loans in the past – or even just visited a payday loan site – and demand payment of debts that don't exist, or aren't owed to that company. Typically, these consumers already face financial challenges, as evidenced by their interest in payday loans. One of my goals this year is to step up our targeting of the companies that sell this data to scam artists.

Our recent case against data broker LeapLab is one example. It is similar to the *Equifax* and *TeleTrack* cases, but alleges more broadly that sale of data to scam artists could violate the FTC Act. Our complaint alleges that LeapLab bought the payday loan applications of financially-strapped consumers – which included their bank account information and Social Security numbers – and then sold them to companies whom it knew had no legitimate need for it.[17] These buyers included phony internet merchants that used the information to withdraw millions of dollars from consumers' accounts without their authorization. We allege that LeapLab's sale of this data to scam artists

17 *FTC v. Sitesearch Corp. d/b/a LeapLab, LLC et al.*, FTC Matter No. 142-3192 (D. Az. filed Dec. 22, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3192/sitesearch-corporation-doing-business-leaplab.

and others with no legitimate need for it is an unfair practice under the FTC Act. This matter is currently in litigation.

There's much more to discuss on this topic and I hope we'll be able to expand on the issues in the panel discussion. But just to plant some seeds: I am well aware that these laws have significant gaps, and are far from a perfect fit for today's marketplace. Notably, most people think wearables and health devices are covered by HIPAA, but they're not. They are, however, covered by the FTC Act. As to the FCRA, it's not always clear where marketing ends and eligibility determinations begin. And the law does not apply to businesses that use their own in-house data analytics to make decisions about their customers or employees. Also, it could be particularly challenging to address biases that are introduced in the research that forms the basis of Big Data. In addition, the ECOA is limited to credit decisions – it does not apply to discrimination in other decisionmaking. However, I think we can make some real progress by educating businesses and the public about what the existing laws do require, enforcing these laws vigorously, and also raising public awareness about what's in the Black Box. At the FTC, we are doing this, using all of the tools at our disposal.