ORBES (Apr. 16, 2012, 12:00PM), http://www.forbes.com/sites/sap/2012/04/16/how-cloud-and-big-data-are-impacting-the-human-genome-touching-7-billion-lives/.

[2] Eilene Zimmerman, *The Race to a $100 Genome*, CNN MONEY (June 25, 2013, 10:43 AM), http://money.cnn.com/2013/06/25/technology/enterprise/low-cost-genome-sequencing/

[3] Public Health Watch, *How A Computer Algorithm Predicted West Africa's Ebola Outbreak Before It Was Announced*, PUBLIC HEALTH WATCH (Aug. 10, 2014), http://publichealthwatch.wordpress.com/2014/08/10/how-a-computer-algorithm-predicted-west-africas-ebola-outbreak-before-it-was-announced/.

[4] Barbara Thau, *How Big Data Helps Chains Like Starbucks Pick Store Locations – An (Unsung) Key To Retail Success*, FORBES (Apr. 24, 2014, 8:49 AM), http://www.forbes.com/sites/barbarathau/2014/04/24/how-big-data-helps-retailers-like-starbucks-pick-store-locations-an-unsung-key-to-retail-success/.

[5] DAVE EGGERS, THE CIRCLE (Alfred A. Knopf 2013).

transparency.[10] In this report we also called attention to the need to focus on a strong technical and contractual framework for deidentifying data that is linkable to individuals, and to develop better ways for consumers to exercise control over sensitive information, such as health information.

Big data holds tremendous promise to solve critical health problems from identifying disease outbreaks[11] to developing personalized medicine.[12] But in order to ensure that this promise is realized, we must address the privacy concerns surrounding use of sensitive health information about individuals. The FTC has begun to take a closer look at the challenges of health information, both in our enforcement work,[13] and in our workshops and research about privacy and security surrounding consumer-generated health data.[14]

The FTC has also taken on another big data arena that has a significant impact on individuals: data brokers. These firms, largely unknown to consumers, collect and combine compendia of billions of bits of innocuous information, and then run them through their big data analytics mill to make predictions about each of us, often based on sensitive personal behavior and characteristics.[15] This data is quite valuable to many companies that want to know where we live, where we work, and how much we earn – as well as our race, our daily activities (both off line and online), our interest

After an in-depth study, the Commission recommended that Congress enact legislation that encompasses both use restrictions for data brokers and their downstream clients, as well as meaningful notice and choice solutions for data broker and their sources of information. Since most consumers have never heard of data brokers, we also call on Congress to enact legislation that would lay out their existence and activities at a consumer-friendly centralized portal, a solution I have long advocated.[16]

The need for accountability at all levels of the data broker industry – including sources, users, and data brokers themselves – is evident when you consider the FTC's finding that some data broker products include race, ethnicity, religion, and national origin as data elements;[17] and some products segment consumers into categories that closely track racial and ethnic categories. These and other big data tools have the potential to promote economic inclusion. For example, big data driven marketing can make underserved consumers aware of opportunities for credit and other services.[18] Conversely, the same data could be used to target advertisements for high-interest payday loans toward financially vulnerable populations.[19] Whether and how consumer profiles based on big data are used to discriminate or treat consumers unfairly involves many subtle and difficult questions.[20] As a recent White House report on big data and social values noted, the line between common practices like offering perks or better deals to loyal customers

[16] *See* Julie Brill, Comm'r, FTC, Sloan Cyber Security Lecture: A Call to Arms: The Role of Technologists in Protecting Privacy in the Age of Big Data (Oct. 23, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/call-arms-role-technologists-protecting-privacy-age-big-data/131023nyupolysloanlecture.pdf *and* Julie Brill, *P*

and practices that "exacerbate existing socio-economic disparities" may be blurry.[21] I am hopeful that the same reservoirs of data that create these concerns will also lead to ways to get them under control. In the past, data has helped identify patterns of discrimination in home mortgage lending,[22] and data has pointed to the absence of discrimination in mainstream credit scoring models.[23] The FTC will host an in-depth discussion of these issues at a public workshop next Monday.[24]

Many of the FTC's counterparts in Europe are examining similar questions about big data, privacy, and economic growth. Many of the findings and recommendations in these reports align with ours at the FTC – further evidence of our common goal. Let me provide a few examples.

Just a couple of months ago, the UK Information Commissioner's Office (ICO) issued a report on *Big Data and Data Protection*.[25] The ICO report presents a frank picture of the challenges that regulators and companies face in the age of big data, including the assertion by some big data enthusiasts that using big data effectively requires collecting "all" the data and leaving open the possibility of using the data for purposes completely unrelated to those for which it was collected. In ICO's view, these are challenges to be solved, not reasons to abandon long-standing data protection principles. As the report states, "[b]ig data is not a game that is played by different rules."[26]

"right to preserve obscurity."[35] The case stems from a Spanish citizen, Mario Costeja González, who complained that searches for his name on Google returned information about attachment proceedings relating to social security debts that he owed.[36]

There was no dispute about whether this information was true. It was. Indeed, the Spanish newspaper that published this information in 1998 was required to do so by the Ministry of Labour and Social Affairs.[37] The attachment proceedings were resolved "for several years" before Costeja González filed his complaint with the Spanish Data Protection Agency.[38]

The ultimate question forwarded from the Spanish court to the ECJ was whether information about the attachment proceedings, sixteen years earlier, should, under the Spanish law transposing the Data Protection Directive,[39] still be associated with searches on the complainant's name.[40] The ECJ decided that Google must keep information about the attachment proceedings out of search results for the complainant's name. More generally, the ECJ held that search engines must not include in search results of this type information that "appear[s] to be inadequate, irrelevant or no longer relevant, or excessive . . . in light of the time that has elapsed" since collection.[41] The court also held, however, that this rule may change for individuals occupying certain roles in public life because of the "preponderant interest of the general public in having, . . . access to the information in question."[42]

This ruling brought about a discrete change in companies' understanding of European law. Beforehand, search engines did not weigh an individual's assessment of the relevance of

---

[35] David Hoffman, *Europe's New Right to be Forgotten: Not New and Not Forgetting*, POLICY@INTEL (July 16, 2014), *available at* http://blogs.intel.com/policy/2014/07/16/europes-new-right-forgotten-new-forgetting/ (positing that the ECJ decision is about a "right to be relevant"); Evan Selinger & Woodrow Hartzog, *Google Can't Forget You, But It Should Make You Hard to Find*, WIRED (May 20, 2014, 3:33 p.m.), http://www.wired.com/2014/05/google-cant-forget-you-but-it-should-make-you-hard-to-find/ (casting the ECJ's *Google* decision as part of a debate about "the proper way to enhance or preserve obscurity"). Another U.S. commenter welcomed the decision as a "pragmatic and flexible" balancing of free expression and privacy interests. Eric Posner, *We All Have the Right to Be Forgotten*, SLATE (May 14, 2014, 4:37 p.m.), http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html (praising the decision because "the type of balancing endorsed by the European Court of Justice.

information returned in connection with searches on his or her name. They now understand that they are under an obligation in the EU to consider requests from individuals to do so. This decision, however, has raised important questions about how this obligation must be fulfilled in a manner that appropriately balances the right of relevancy with "the right of the public in having . . . information" about individuals[43] and, more generally, freedom of expression.[44] – a balance that will take time to strike. Here are a few of the questions that I expect to come up along the way:

> What time period will determine whether a piece of information is relevant? For instance, what if only ten years had elapsed between the publication of information in the Google case and the ECJ's decision, rather than 16? What about five years?
>
> How should search engines assess relevance when users enter searches that are more focused than someone's name? For example, does a search engine have

credit grantors, insurance companies, employers, landlords, and other entities in making eligibility decisions affecting consumers.[46]

The Fair Credit Reporting Act contains a relevance requirement. After a certain period of time – seven years in most cases – information about debt collections, civil lawsuits, tax liens, and even arrests for criminal offenses become "obsolete"[47] and must be taken out of consumer reports.[48] This requirement in the FCRA advances Congress's purpose of "fairness, impartiality, and a respect for the consumer's right to privacy."[49] In effect, this part of the law reflects the judgment of our Congress that information about an unpaid bill or even an arrest should not follow people around for the rest of their lives in their consumer reports, balanced against the need for relevant information in the context of granting credit and making other decisions that are subject to the FCRA. This policy judgment was upheld as providing sufficient protections for First Amendment interests.[50]

I have called for putting similar controls in the hands of consumers where data is used for marketing and other purposes not covered by the FCRA. As part of my "Reclaim Your Name" initiative, I call on data brokers to empower the consumer to find out how brokers are collecting and using her data; give her access to information that data brokers have amassed about her; allow her to opt-out if she learns a data broker is selling her information for marketing purposes; and provide her the opportunity to correct errors in information used for substantive decisions.[51] These choices would allow consumers to keep aspects of their personal make-up away from big data driven marketing – something that will be increasingly important as more and more sensitive information about consumers becomes available.

The Internet, of course, has radically transformed the process by which data brokers, advertising networks, third-party analytic firms and others gather information about individuals.[52] For example, "people search" services allow users to search for publicly available

[46] *See* 15 U.S.C. § 1681a(d) (defining "consumer report"); see also FTC, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT 1 (2011) (staff report), *available at* http://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf. The FCRA also regulates persons who furnish information