Privacy in the Age of Omniscience:
Approaches in the United States and Europe

U.S. Federal Trade Commissioner Julie Brill
Mentor Group Vienna Forum
September 11, 2014

Good afternoon, and thank you to Tom Kosmo and the Mentor Group for inviting me to address you today. I am delighted to provide some perspective on developments in privacy in the United States and Europe.

Today, we live in a world awash in data and opportunity. As we traverse the first decades of the 21st century, we are moving much of our lives online, demanding – and receiving – more powerful, more mobile, faster, and multifaceted connections. It seems that every day – perhaps every hour – new innovations and technologies open new avenues for us to obtain, collect, parse, and share information.

Let's put these advances in the context of healthcare. One of the greatest scientific discoveries of our generation is the mapping of the human genome. That project, completed in 2003, took thirteen years and cost billions of dollars.[1] In 2007, the first individual genomes were sequenced; the price tag was about a million dollars. Today, you can have your genome sequenced for between $1000 and $4000, and scientists predict we will see $100 individual genome sequencing in the next few years.[2]

And that is just one example of how burgeoning big data is altering the face of health care – and public policy, business, city planning, child rearing – you name it. Smart cars are making our traffic smoother and our streets safer. Public health emergencies, from the flu to Ebola, are predicted and managed with information from big data algorithms.[3] Companies like Starbucks and the fast food chain Wendy's are locating their stores based on cyber-sifting through troves of demographic information.[4]

We are on the threshold of an age in which, as Dave Eggers's "Circlers" would say, "all that happens will be known."[5] Some are so sure that this Age of Omniscience will be a golden

---

[1] Jacqueline Vanacek, *How Cloud and Big Data Are Impacting the Human Genome – Touching 7 Billion Lives*, FORBES (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).

one, that raising concerns about consumer protection and privacy seems to them almost quaint – if not futile.[6]

Not among many of you here today, I know. It is once again a pleasure to speak to fellow jurists and regulators here in Europe. Often when I give talks, I have to spend half my time making the case that privacy in a big data world is both possible and worth fighting for. Here, you take it as given that privacy is, in the words of U.S. Supreme Court Justice Louis Brandeis almost ninety years ago, "the most comprehensive of rights and the right most valued by civilized men."[7] Here, we can all agree that as the Age of Omniscience descends upon us, we can and will find ways to protect individual privacy.

That much is clear. How we get there is less so. And how quickly we get there – or are expected to get there, in these times when the Internet has made a secular faith of rapid change – is also unclear. I do have to believe, though, it will not be in the click of a mouse. As Konrad Adenauer has been widely quoted as saying: "In an instant age, perhaps we must relearn the ancient truth that patience, too, has its victories."[8]

We need to cleave to this wisdom as we make our way over a shifting and volatile terrain. Though we may take somewhat different paths in the U.S. and the EU, we are all taking the same journey, and seeking to reach the same place: An Age of Omniscience complete with a meaningful right to privacy.

Transatlantic Efforts to Reconcile Big Data and Privacy

My agency, the U.S. Federal Trade Commission, has, through enforcement actions and forward-looking policy development, been exploring the issue of privacy in a data-intensive world for the past several years.

Beginning in 2009, we have held a series of public roundtables and collected written comments to help determine whether the privacy framework that had guided us in the past was up to the task for this decade.[9] This work culminated in our release of a landmark report in which we articulated the best practices of privacy by design, simplified choice, and greater

---

[6] *See, e.g.*, Craig Mundie, *Privacy Pragmatism: Focus on Data Use, Not Data Collection*, 93 FOREIGN AFFAIRS 28, 29 (2014) (arguing that "the era of 'big data' . . . has rendered obsolete the current approach to protecting individual privacy and civil liberties" and that regulators and lawmakers should "shift[] the focus from limiting the collection and retention of data to controlling data at the most important point—the moment when it is used").

[7] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[8] Adenauer is widely cited as the source of this statement. *See, e.g.*, Konrad Adenauer, WIKIQUOTE, http://en.wikiquote.org/wiki/Konrad_Adenauer (last updated Apr. 13, 2014). It appears, however, that the source of this quotation is Gabriel Hauge, *Interdependence and the First World*, 14 ATLANTIC COMMUNITY QUARTERLY 195, 200 (Summer 1976), thus demonstrating that the Age of Omniscience may yet have a few gaps!

[9] *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 22-38 (preliminary staff report) (Dec. 2010), *available at* http://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

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 interests, our health conditions and our financial status.

---

[10] *See generally* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[11] *See supra* note 3.

[12] *See* Karen Weintraub, *Firm Hopes Big Data Can Personalize Health Care*, BOSTON GLOBE (May 13, 2013), http://www.bostonglobe.com/business/2013/05/12/personalized-medicine-goal-big-data-scientist/28gTkXjCDj6Zh6KP5tpNBO/story.html (discussing the use of "information aggregated from thousands of cases . . . to determine what treatment made the crucial difference for each patient, and with it what is likely to work best for the next patient").

[13] *See generally* GMR Transcription Svcs., Inc., Case No. C-4482 (F.T.C. Aug. 14, 2014) (decision and order), *available at* http://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf; Accretive Health, Inc., Case No. C-4432 (F.T.C. Feb. 5, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140224accretivehealthdo.pdf; CBR Sys., Inc., Case No. 4400 (F.T.C. Apr. 29, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/05/130503cbrdo.pdf; Epic Marketplace, Inc. Case No. 4389 (F.T.C. Mar. 13, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/03/130315epicmarketplacedo.pdf.

[14] *See* Federal Trade Commission Workshop on Consumer Generated and Controlled Health Data Seminar 26-27 (May 7, 2014), available at http://www.ftc.gov/news-events/events-calendar/2014/05/spring-privacy-series-consumer-generated-controlled-health-data; Jared Ho, Comments at Federal Trade Commission Consumer Generated and Controlled Health Data Seminar 26–27 (May 7, 2014), *available at* http://www.ftc.gov/system/files/documents/public_events/195411/2014_05_07_consumer-generated-controlled-health-data-final-transcript.pdf.

[15] FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 20, 25 & nn.52, 57, (2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [DATA BROKER REPORT].

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, Comm'r, FTC, Keynote Address at the 23rd Computers, Freedom, and Privacy Conference: Reclaim Your Name (June 26, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/reclaim-your-name/130626computersfreedom.pdf. .

[17] DATA BROKER REPORT, *supra* note 15, at B-3.

[18] *See* FTC, Conference Description, Big Data: A Tool for Inclusion or Exclusion?, http://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion (last visited Sept. 5, 2014) ("[U]ses of big data are expected to create efficiencies, lower costs, and improve the ability of certain populations to find and access credit and other services."). *See also* Comment of the Chamber of Commerce of the United States on the Big Data: A Tool for Inclusion or Exclusion? Workshop 3 (Aug. 15, 2014), available at http://www.ftc.gov/system/files/documents/public_comments/2014/08/00021-92389.pdf (quoting with approval the FTC's conference description).

[19] *See, e.g.*, Comment of the National Consumer Law Center on the Big Data: A Tool for Inclusion or Exclusion? Workshop 2 (Aug. 15, 2014), *available at* http://www.ftc.gov/system/files/documents/public_comments/2014/08/00018-92374.pdf; Jeffrey Chester and Edmund Mierzwinski, Big Data Means Big Opportunities and Big Challenges: Promoting Financial Inclusion and Consumer Protection in the "Big Data" Financial Era 13 (Mar. 2014) (submitted as a comment of the Center for Digital Democracy and U.S. PIRG on the Big Data: A Tool for Inclusion or Exclusion? Workshop), *available at* http://www.ftc.gov/system/files/documents/public_comments/2014/05/00003-90097.pdf.

[20] *See* Michael Schrage, *Big Data's Dangerous New Era of Discrimination*, HARVARD BUSINESS REVIEW BLOG NETWORK (Jan. 29, 2014, 8:00 a.m.), http://blogs.hbr.org/2014/01/big-datas-dangerous-new-era-of-discrimination/ (arguing that "Big Data — and its associated analytics — dramatically increase both the dimensionality and degrees of freedom for detailed discrimination" and urging companies to "use Big Data analytics to justify their segmentation/personalization/discrimination strategies").

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] ICO's recommendations – including improving notice and choice mechanisms, exploring realistic uses of deidentification, and practicing privacy by design – all align quite well with what the FTC has recommended.

A second example is the European Commission's Digital Agenda and its recent Communication on a data-driven economy.[27] The Communication notes that we are

---

[21] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 46-47 (2014), *available at* http://www.whitehouse.gov/sites/default/files/. docs/big_data_privacy_report_may_1_2014.pdf.

[22] *See* Peter P. Swire, *The Persistent Problem of Lending Discrimination: A Law and Economics Analysis*, 73 TEX. L. REV. 787, 806-14 (1995) (reviewing empirical evidence and concluding that "significant lending discrimination" existed at the time the article was published).

[23] *See* BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, REPORT TO CONGRESS ON CREDIT SCORING AND ITS EFFECTS ON THE AVAILABILITY AND AFFORDABILITY OF CREDIT S-1 – S-2 (Aug. 2007), *available at* http://www.federalreserve.gov/boarddocs/rptcongress/creditscore/creditscore.pdf (concluding that "the credit characteristics included in credit history scoring models do not serve as substitutes, or proxies, for race, ethnicity, or sex").

[24] *See* FTC, Conference Description, Big Data: A Tool for Inclusion or Exclusion?, http://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion (last visited Sept. 5, 2014).

[25] UK INFORMATION COMMISSIONER'S OFFICE, BIG DATA AND DATA PROTECTION (July 28, 2014, v. 1.0), *available at* http://ico.org.uk/news/latest_news/2014/~/media/documents/library/Data_Protection/Practical_application/big-data-and-data-protection.pdf.

[26] *Id.* at 4.

[27] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, *Towards a Thriving Data-Driven Economy* (July 2, 2014), *available at* https://ec.europa.eu/digital-agenda/en/news/communication-data-driven-economy.

"witness[ing] a new industrial revolution driven by digital data, computation and automation" that can transform transportation, healthcare, and energy and resource conservation.[28] Fully exploiting the data in these sectors not only requires having analytical know-how but also ensuring that "[u]sers have sufficient trust in the technology, the behaviors of providers, and the rules governing them."[29] The Communication concludes that complying with data protection rules, and incorporating practices such as deidentification and privacy by design, are ways to build this trust.[30]

Finally, the European Data Protection Supervisor recently observed that "there appears to be a blurring of the line between consumer protection and competition."[31] The report argues that "competition policy must . . . be vigilant in case dominant companies use personal data to gain further advantage over their competitors."[32] As a consumer protection and privacy official who also wears a competition hat in the United States, I can attest that the Commission has taken action where we have had concerns about competitive effects of combining data held by merging companies,[33] and we will continue to examine this important area going forward.[34]

All of these efforts illustrate the search by regulators for answers about how to reconcile the furious pace of growth in big data analytics with more stable values such as privacy and fair treatment. But regulators are not the only actors who will play a critical role in forging the path to reconciling big data and privacy. The European Court of Justice's decision in *Google Spain v. AEPD* provides an example of the important role of the courts and how their decisions – based on the particular facts and legal issues presented in any particular case – require patience in order to be fleshed out in the fullness of time.

Persistence Versus Relevance

The ECJ's *Google* decision, in my view, was not about a "right to be forgotten." Instead, as some commenters on my side of the Atlantic observed, it is about a "right of relevancy" or a

---

[28] *Id.* at 3.

[29] *Id.* at 5.

[30] *Id.* at 11.

[31] EUROPEAN DATA PROTECTION SUPERVISOR, REPORT OF WORKSHOP ON PRIVACY, CONSUMERS, COMPETITION AND BIG DATA 4 (July 11, 2014), *available at* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Big%20data/14-07-11_EDPS_Report_Workshop_Big_data_EN.pdf.

[32] *Id.* at 3.

[33] *See* CoreLogic, Inc., Case No. C-4458 (F.T.C. May 20, 2014) (decision and order), *available at* http://www.ftc.gov/system/files/documents/cases/140521corelogicdo.pdf; Fidelity National Financial, Inc., No. C-4425 (Mar. 4, 2014) (decision and order), *available at* http://www.ftc.gov/system/files/documents/cases/140305fidelitdo.pdf.

[34] Julie Brill, Comm'r, FTC, Address Before the European Data Protection Supervisor's Workshop on Privacy, Consumer Protection, and Competition in the Digital Age: Weaving a Tapestry to Protect Privacy and Competition in the Age of Big Data (June 2, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/313311/140602edpsbrill2.pdf.

"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. Privacy allows us to experiment, make mistakes, and start afresh if we mess up").

Some have argued that the ECJ decision is wrong on policy, and an affront to the First Amendment. *See, e.g.*, Ann Cavoukian & Christopher Wolf, *Sorry, But There's No Online Right to Be Forgotten*, FULL COMMENT, NATIONAL POST (June 25, 2014, 12:01 ET).

[36] Google Spain SL v. Agencia Española de Proteccíon de Datos ¶ 14, (Court of Justice of the European Union, Case C 131/12), *available at* http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-131/12&td=ALL [*Google v. AEPD*].

[37] *Id.* at ¶ 16.

[38] *Id.* at ¶¶15-16.

[39] *Id.* ¶ 13. The relevant Spanish law is Organic Law Number 15/1999 of December 13, 1999. *Id.*

[40] Before ruling on this question, the court held that Google and its Spanish subsidiary were subject to the jurisdiction of Spanish courts and that Google is a data controller in its capacity as the operator of a search engine.

[41] *Google v. AEPD* at ¶ 93.

[42] *Id.* at ¶ 97.

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 more latitude to return information in response to the query "Julie Brill tax deadbeat" rather than a search for simply "Julie Brill"? Does the answer change if I make this request years after retiring from the public stage?

- Does the ECJ's decision cover a newspaper's own search engine that returns results ranked by relevance?

- Does the decision apply to entities other than search engines, such as newspapers that were not required by law to publish the original information?

- Do the obligations identified in the decision apply outside the EU?

Many in the United States viewed the ECJ's decision as a major new development, and some have raised concerns that it is an affront to concepts imbedded in our shared values of freedom of expression.[45] These are clearly important issues to consider. As we do so, I urge thought leaders on both sides of the Atlantic to recognize that, just as we both deeply value freedom of expression, we also have shared values concerning relevance in personal information in the digital age.

A U.S. Perspective on Relevance: "Obsolete" Information and Individual Profiles

One of the oldest and most important privacy laws we have in the United States is the Fair Credit Reporting Act (FCRA). Enacted in 1970, the FCRA regulates the practices of entities that collect and compile consumer information into individualized reports for use by

[43] *Id. at* ¶ 80.

[44] *See id.* at ¶ 9 (referring to Article 9 of the EU Data Protection Directive, "Processing of personal data and freedom of expression").

[45] See *supra* note 35 for a range of reactions, from approving to critical, to the ECJ's decision.

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 for such reports and those who use consumer reports to make eligibility determinations.

[47] *See* Brief of Amici Curiae Consumer Financial Protection Bureau and Federal Trade Commission Supporting Reversal, Moran v. The Screening Pros, LLC, Case No. 2-12-cv-05808 (3d Cir., Oct. 4, 2013) (referring to 15 U.S.C. § 1681c's subject as "Obsolete Information").

[48] 15 U.S.C. § 1681c.

[49] 15 U.S.C. § 1681(a)(4).

[50] *See* Trans Union Corp. v. FTC, 245 F.3d 809, 818-19 (D.C. Cir. 2001).

[51] *See supra* note 16. *See also* Cory Bennett, *Google Official Sees U.S. Slowly Addressing Right to Be Forgotten Through "Miniature Laws,"* WASH. INTERNET DAILY (Sept. 8, 2014) (reporting on industry representatives' mention of Reclaim Your Name and other possible steps, including legislation, to address control over "particular types of information").

[52] *See* Julie Brill, Comm'r, FTC, Concurring Statement in the Matter of US Search, Inc. and US Search, LLC 1 (F.T.C. No. C-4317, Mar. 25, 2011), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110325ussearchstatementbrill.pdf ("The advent of the Internet and high-speed data transfers has dramatically increased data brokers' ability to gather public information from just about any source imaginable. Data brokers can now use sophisticated computer algorithms to

information about consumers.[53] These records can provide an unsettlingly comprehensive look at individuals' lives, including the names of their relatives, their employment histories, and property ownership and divorce records.[54]

The Federal Trade Commission believes that more uniform rules are needed for this broader category of people search services. In our data broker report, we recommended that Congress consider legislation requiring people search providers to allow consumers to opt out, to disclose the limitations of such an opt out, and to reveal their sources of information so that consumers can correct inaccurate information.[55] Like the FCRA, the people search legislation we recommend would apply to a specific type of information service and define specific obligations to allow consumers to exercise greater control over information about their lives, present and past.[56]

Institutions for Addressing Privacy Challenges

I firmly believe that we at the FTC need to work with Congress and private sector stakeholders to develop legislation on consumer privacy, data security, and data brokers. In the meantime, we will continue to use the enforcement and policymaking tools that Congress has given us to develop consumer protections case-by-case, one step at a time.

The ECJ's *Google* decision, which provoked such passionate discussion in the U.S. and Europe, also provides an opportunity to tackle privacy issues through an incremental, case-by-case approach. After years in which officials on both sides of the Atlantic have downplayed the role of decisions in specific cases, we may find that the ECJ's decision draws national courts, data protection authorities, and others into a robust and healthy discussion about how to apply the court's interpretation of the Directive – and the "right of relevancy" – to new facts.

In other words, the work of defining the contours of a "right to relevance" is not done. To understand the full scope of the ECJ's decision, we will have to take the longer view. U.S. courts, prosecutors, and the defense bar have long been accustomed to this approach as they work through the meaning of Supreme Court decisions interpreting the contours of the Fourth Amendment's prohibition against unreasonable searches and seizures, including recent decisions

---

piece together countless bits of discrete public data – sometimes combined with nonpublic information – into a composite consumer profile that many would find unsettling in its comprehensiveness. Understandably, many consumers want to have the choice to opt out of such data gathering, processing, and use, at least for certain purposes, such as marketing.").

[53] DATA BROKER REPORT, *supra* note 15, at iii.

[54] *Id.* at 34; Julie Brill, Comm'r, FTC, Concurring Statement in the Matter of US Search, Inc. 1 (Mar. 25, 2011), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/concurring-statement-commissioner-julie-brill/110325ussearchstatementbrill.pdf.

[55] DATA BROKER REPORT, *supra* note 15, at 54.

[56] Along related lines, the FTC's order against Facebook requires the company to "implement procedures reasonably designed to ensure that covered information cannot be accessed by any third party from servers under Respondent's control after a reasonable period of time, not to exceed thirty (30) days, from the time that the user has deleted such information or deleted or terminated his or her account," with certain limited exceptions. Facebook, Inc., Case No. C-4365 at 5 (July 27, 2012).

interpreting these rights in an advanced technological age that includes GPS tracking devices[57] and smartphones.[58] Similarly, those who must apply the ECJ decision – Internet search firms, and perhaps newspapers with search engines, and other companies– must have "patience" as the national courts and data protection authorities flesh out the ECJ's pronounced principle of relevance in the context of search. And legislative bodies, policymaking agencies, individual companies, and self-regulatory bodies could all play a constructive role in filling in the details.

The issue of relevancy and fairness with respect to information about individuals in this advanced technological age is just one of the issues that will require patience – and persistence – in Europe and the United States. As we go about our common work protecting and nurturing a clear right to privacy within the new world of big data, economic growth, and technological change, we should keep in mind the words of Voltaire: "Trees that are slow to grow bear the best fruit." And we should not forget we are travelling into the Age of Omniscience – if not exactly together in lock step – then certainly together in the values that drive us forward.

[57] United States v. Jones, 132 S. Ct. 945 (2012) (holding that the placement of a GPS tracking device on a suspect's vehicle outside the restrictions specified in a warrant, and subsequent collection of location information from the tracking device, constituted an unconstitutional search).

[58] Riley v. California, 143 S. Ct. 2473 (2014) (holding that law enforcement officers generally must obtain a warrant to search a cell phone obtained from a suspect pursuant to a lawful arrest).