



Jessica L. Rich  
Office of the Director  
Bureau of Consumer Protection

UNITED STATES OF AMERICA  
Federal Trade Commission  
WASHINGTON, D.C. 20580

August 1, 2014

By Electronic Filing

National Telecommunications and Information Administration  
U.S. Department of Commerce  
1401 Constitution Avenue N.W.  
Washington, DC 20230

Re: Comment: Big Data, Consumer Privacy, and the Consumer Bill of Rights

Dear National Telecommunications and Information Administration:

As the Director of the Federal Trade Commission's Bureau of Consumer Protection, I appreciate this opportunity to respond to your June 4, 2014 request for comment ("Request for Comment") regarding how developments in "Big Data" affect consumer privacy and the interests reflected in the Administration's Consumer Privacy Bill of Rights.<sup>1</sup>

While definitions of "Big Data" vary, the term is often used, as I use it here, to refer to a confluence of factors, including the ubiquitous collection of consumer data via the Internet, social media, mobile devices, and sensors; the plummeting cost of storing such data; and powerful new capability to analyze such data to draw connections and make inferences and predictions. As the nation's leading consumer privacy enforcement agency, the FTC has addressed the privacy implications of Big Data through its law enforcement and policy work, and will continue to focus on these issues as part of its consumer protection mission.

The FTC's focus on privacy dates back to enactment of the Fair Credit Reporting Act ("FCRA") in 1970.<sup>2</sup> The FTC has been the primary enforcer of this law, which protects

---

<sup>1</sup> The views expressed in this letter are my own and do not necessarily reflect the views of the Federal Trade Commission or any particular Commissioner.

<sup>2</sup> 15 U.S.C. §§ 1681-1681x (2012).

sensitive consumer report information – that is, data used for decisions involving credit, employment, insurance, and other eligibility determinations – from disclosure to unauthorized persons.

Beginning in the mid-1990s, the FTC began to examine consumer privacy issues extending beyond the concerns reflected in the FCRA. The Commission’s primary source of legal authority is Section 5 of the FTC Act,<sup>3</sup> which empowers the Commission to take action against deceptive or unfair practices. The Commission also enforces numerous sector-specific statutes, including the Gramm-Leach-Bliley Act,<sup>4</sup> the Children’s Online Privacy Protection Act,<sup>5</sup> the CAN-SPAM Act,<sup>6</sup> and the Telemarketing and Consumer Fraud and Abuse Prevention Act and the associated Do Not Call Rule.<sup>7</sup> Under these laws, the Commission has brought a variety of privacy-related cases, including cases against companies engaged in Big Data analytics, such as Twitter, Google, and Facebook. The FTC also educates consumers and businesses, conducts studies, testifies before Congress, hosts public events, and writes reports regarding the privacy and security implications of technologies and business practices that affect consumers. Recently, much of the FTC’s privacy work has addressed Big Data issues.

My comment begins by summarizing this recent FTC body of work. It then discusses some of the benefits and privacy risks associated with Big Data. Finally, in response to questions posed in the Request for Comment, the comment explains why de-identification, accountability mechanisms, and the “notice and consent” model remain vital tools to protect consumer privacy in a Big Data era.<sup>8</sup>

## A. **FTC INITIATIVES RELATING TO BIG DATA**

### 1. **Exploration of Emerging Issues**

Over the past several years, the Commission has hosted a number of workshops addressing the proliferation of Big Data and its privacy ramifications. In 2009 and 2010, the Commission hosted a series of public roundtables examining the myriad ways in which companies can amass “little data” from consumers and turn it into comprehensive databases and

---

<sup>3</sup> 15 U.S.C. § 45.

<sup>4</sup> Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.).

<sup>5</sup> 15 U.S.C. §§ 6501–6506 .

<sup>6</sup> 15 U.S.C. §§ 7701-7713.

<sup>7</sup> 15 U.S.C. §§ 6101-6108

<sup>8</sup> The Commission discussed these approaches its Privacy Report and the White House addressed them its recent report on Big Data. *See* FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012) [hereinafter PRIVACY REPORT], *available at* <http://ftc.gov/os/2012/03/120326privacyreport.pdf>; EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES, *available at* [http://www.whitehouse.gov/sites/default/files/docs/big\\_data\\_privacy\\_report\\_5.1.14\\_final\\_print.pdf](http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf) (2014).

detailed consumer profiles.<sup>9</sup> In particular, the roundtables examined the ways in which companies collect data from consumers, including through social networking sites, mobile devices, and contracts with data brokers. Based on the roundtables, the Commission issued its Privacy Report setting forth a generally-applicable framework for addressing consumer privacy issues. In the report, the Commission encouraged companies to adopt the following three core approaches to consumer privacy:<sup>10</sup>

- *Privacy-by-Design.* Build in privacy at every stage of product development by incorporating substantive privacy protections into business practices – such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy – so that privacy is part of the fundamental business model and not overlooked or added later as an afterthought.
- *Streamlined Choice for Businesses and Consumers.* Give consumers the ability to make decisions about their data at a relevant time and context, while eliminating the burden of providing choice for data practices that are obvious or consistent with consumers’ reasonable understanding and expectations. In certain contexts, this will mean “just-in-time” notice.
- *Greater Transparency.* Make sure that information collection and use practices are transparent to consumers, such as by giving consumers reasonable access to their information and by standardizing and improving privacy policies.

More recently, in November 2013, the Commission held a public workshop to explore an emerging form of consumer data collection – through sensors placed in everyday devices that connect to the Internet, a phenomenon known as “the Internet of Things.” Participants discussed the privacy issues raised by the Internet of Things – including the increased ubiquity and invisibility of data collection, the challenges of providing notice and choice in a “no screen” environment, and what incentives exist for designing products with privacy and security in mind. Materials from the workshop, including video and transcripts, are available on the FTC website<sup>11</sup> and the Commission plans to issue a report on the workshop in the coming months.

In the spring of 2014, the FTC also hosted a series of seminars to examine the privacy implications of three new technologies and business models that further enable companies to

---

<sup>9</sup> See Press Release, Fed. Trade Comm’n, FTC to Host Public Roundtables to Address Evolving Consumer Privacy Issues (Sept. 15, 2009), available at <http://www.ftc.gov/news-events/press-releases/2009/09/ftc-host-public-roundtables-address-evolving-consumer-privacy>.

<sup>10</sup> See PRIVACY REPORT, supra note 8, at 15-72.

<sup>11</sup> Fed. Trade Comm’n, Internet of Things – Privacy and Security in a Connected World (Nov. 19, 2013), available at <http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world>.

gather Big Data about consumers: (1) mobile device tracking of consumers as they move within and among retail stores and other brick-and-mortar businesses (2) predictive score modeling, through which companies can determine consumers' likely response to product and service offers, and (3) consumer generated and controlled health data that is not covered by the Health Insurance Portability and Accountability Act. The series featured academics, business and industry representatives, and consumer advocates for two-hour discussion sessions, as well as a request for public comments. Materials from the seminars, including video and transcripts, are available on the FTC website.<sup>12</sup>

Finally, in April, the FTC announced a public workshop entitled "Big Data: A Tool for Inclusion or Exclusion?" to be held on September 15, 2014, to further explore the use of Big Data and its potential impact on American consumers, including low income and underserved consumers.<sup>13</sup> The workshop will bring together academics, business and industry representatives, and consumer advocates to discuss the following issues:

- How are organizations using Big Data to categorize consumers?
- What benefits do consumers gain from these practices? Do these practices raise consumer protection concerns?
- What benefits do organizations gain from these practices? What are the social and economic impacts, both positive and negative, from the use of big data to categorize consumers?
- How do existing laws apply to such practices? Are there gaps in the legal framework?
- Are companies appropriately assessing the impact of big data practices on low income and underserved populations? Should additional measures be considered?

Many of these issues overlap with questions posed in the Request for Comment.

## **2. FTC Data Broker Report**

In May 2014, the Commission issued *Data Brokers: A Call for Transparency and Accountability* to shed light on the data broker industry and its practices ("Data Broker Report").<sup>14</sup> As noted in the report, data brokers are important participants in the Big Data ecosystem because they can aggregate a wealth of consumers' personal information from disparate sources, categorize it, and resell or share that information with others. The report

---

<sup>12</sup> See Press Release, Fed. Trade Comm'n, FTC to Host Spring Seminars on Emerging Consumer Privacy Issues (Dec. 2, 2013), available at <http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues>.

<sup>13</sup> Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion (Sept. 19, 2014), available at <http://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion>.

<sup>14</sup> FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014) [hereinafter DATA BROKER REPORT], available at <http://ftc.gov/os/2012/03/120326privacyreport.pdf>.

discusses the results of an in-depth study of the data collection and use practices of nine data brokers, which represent a cross-section of the industry. The data brokers that were studied collect personal information about consumers from a wide range of sources and provide it for a variety of purposes, including verifying an individual’s identity, marketing products, providing “people search” websites through which users can search for publicly available information about consumers, and detecting fraud. Moreover, the report found that data brokers combine and analyze data about consumers to make inferences about them, placing them in categories as innocuous as “Dog Owner” or as potentially sensitive as “Urban Scramble” or “Mobile Mixers,” both of which included a high concentration of Latinos and African Americans with low incomes. Because these companies generally never interact with consumers, consumers are often unaware of their existence, much less the wealth of information they collect and the variety of practices in which they engage.

Based on findings from the study, the Commission encouraged Congress to consider enacting legislation to create a centralized mechanism, such as an Internet portal, where data brokers would describe their information collection and use practices and offer links to opt-out tools and tools to provide consumers with reasonable access to information held about them.<sup>15</sup> The report also recommended that such legislation require consumer-facing entities, such as retailers, to provide prominent notice to consumers when they share information with data brokers, along with the ability to opt-out of such sharing. The report further recommended that any legislation require consumer-facing entities to obtain affirmative express consent from consumers before sensitive information, such as health information, is collected and shared with data brokers. The full report, which is available on the FTC’s website, contains more detailed legislative and best practice recommendations. These recommendations address the NTIA’s inquiry about whether additional legal safeguards are warranted with regard to data brokers.<sup>16</sup>

### **3. Law Enforcement**

The FTC has brought hundreds of cases involving privacy and data security. Collectively, these cases have resulted in enhanced privacy protection for well over a billion consumers worldwide and have sent an important signal to businesses about the need to collect and use consumer data responsibly. Many of these cases involve the collection of detailed information about consumers, the storage of consumer information in comprehensive databases, and the collection and use of data by companies that are behind the scenes and unknown to consumers – all issues of significance in today’s Big Data economy. For example, in its recent cases against data brokers Spokeo and Instant Checkmate, the FTC alleged that the companies compiled extensive web-based profiles about consumers, which they marketed to employers for

---

<sup>15</sup> *Id.* at 49-54.

<sup>16</sup> *See* NTIA, Big Data and Consumer Privacy in the Internet Economy, Request for Public Comment, 79 Fed. Reg. 32714, 32715 (June 6, 2014) (question 8).

use in making employment decisions. Accordingly, they were subject to FCRA requirements, such as notifying employers of their obligation to provide an adverse action notice if someone was denied a job based on the companies' data. The FTC complaint alleged that, by not complying with these requirements, the companies violated the FCRA.<sup>17</sup>

Another recent case involved allegedly false claims by mobile messaging app Snapchat that text messages sent through its messaging service would disappear after a certain amount of time. In fact, users of the service were able to employ many different tools to save the messages, as Snapchat knew or should have known. As such, the FTC alleged the company engaged in a deceptive practice by representing to consumers that their text messages would disappear.<sup>18</sup>

And the FTC's over 50 data security cases address alleged failures by a wide range of companies to provide reasonable security for consumer data, an issue that has become increasingly important as companies collect and store more sensitive data than ever before. For example, in the FTC's recent case against TRENDnet, Inc. – also its first Internet of Things case – the FTC alleged that the manufacturer of Internet Protocol cameras failed to maintain reasonable security, in violation of Section 5 of the FTC Act. Among other things, the FTC alleged that the company failed to appropriately test its product, resulting in hackers being able to post private video feeds of people's bedrooms and children's rooms on the Internet.<sup>19</sup>

## **B. BENEFITS AND RISKS OF BIG DATA**

In all of its work, the Commission has highlighted the many benefits of Big Data to consumers. Companies use consumers' information to innovate and deliver better products and services to consumers – for example, smartphones that deliver the latest personalized news stories and connect consumers with friends on social media; home automation systems that know when you are leaving work and when to turn on your front-porch light; and ankle monitors that share with your friends how far you have biked or run at any given moment. Big Data also can be used to enhance more traditional products and services. For instance, data brokers can use Big Data analytics to provide granular marketing lists to brick-and-mortar retailers, which provide consumers with more relevant coupons for the goods and services they want, just when

---

<sup>17</sup> See Complaint, *United States v. Instant Checkmate, Inc.*, No. 14-CV0675-H-JMA (S.D. Cal. Mar. 24, 2014), available at <http://www.ftc.gov/enforcement/cases-proceedings/122-3221/instant-checkmate-inc>; Complaint, *United States v. Spokeo, Inc.*, No. CV12-05001-MMM-SH (C.D. Cal. June 7, 2012), available at <http://www.ftc.gov/enforcement/cases-proceedings/1023163/spokeo-inc>. The FCRA is an important tool to address the use of Big Data for decisions involving credit, employment, insurance, and other eligibility determinations.

<sup>18</sup> See Proposed Complaint, *Snapchat, Inc.*, File No. 132 3078 (F.T.C. May 8, 2014), available at <http://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter>.

<sup>19</sup> See Complaint, *TRENDnet, Inc.*, No. C-4426 (F.T.C. Sept. 4, 2013), available at <http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter>.

they are ready to buy them. Big Data also provides benefits beyond the marketing sphere, such as improving algorithms for determining whether a transaction is fraudulent.

At the same time, Big Data creates privacy risks to consumers, including: (1) unexpected and undisclosed uses of consumer data (2) security risks, and (3) concerns about discriminatory or unlawful data uses. As to lack of transparency, the FTC's Data Broker Report highlights the concerns associated with companies maintaining rich profiles about consumers without their knowledge or consent. The report shows that data brokers acquire and store billions of data elements covering nearly every U.S. consumer from numerous commercial, government, and other public sources. Data brokers then analyze this data to make inferences about consumers, some of which may be considered quite sensitive, and share the information with clients in a range of industries, all without consumers' knowledge and consent.

Second, the proliferation of Big Data creates data security risks. Of greatest concern, the storage of Social Security numbers, financial account numbers, usernames and passwords, and other information can lead to identity theft. But identity thieves and other unscrupulous actors also may be able to exploit the sheer volume and richness of consumer profiles available in today's Big Data economy. These profiles can give these actors a clear picture of consumers' habits over time, thereby enabling them to predict passwords, challenge questions, or other authentication credentials in order to perpetrate identity theft or basic fraud. As illustrated by the TRENDnet case, discussed above, the compromise of Big Data can also reveal sensitive information about people's homes, their children, and their whereabouts. It is clear that, if companies do not protect the consumer data they collect and store, serious harm could occur.

Finally, in the absence of clear norms and expectations surrounding the use of Big Data, there are risks that Big Data may be used in discriminatory or unlawful ways. For example, while a new and improved risk-management product can be used to prevent fraud, it also can be used to limit the ability of a legitimate actor to complete a particular transaction. And while a marketing product can be used to send highly-targeted advertising, it also can be used in discriminatory ways. From our data broker study, we learned that data brokers combine and analyze data about consumers to make inferences about them, including potentially sensitive inferences related to ethnicity, income, religion, political leanings, age, and health conditions. Some consumers may find it troubling to receive advertisements based on their inclusion in these categories. And they would likely find it even more troubling if a company used these categories to decide whether to provide them credit, insurance, employment or other benefits. For example, an insurance company could use the fact that a consumer is a biker, a smoker, or a person interested in diabetes information to infer that the consumer engages in risky behavior.<sup>20</sup>

---

<sup>20</sup> If the data broker's activities do not meet the definition of a "consumer reporting agency," as defined by the FCRA, these uses of the data would not trigger FCRA protections.

Our recent seminar on alternative scoring products highlighted similar concerns about the uses and misuses of Big Data. As discussed at the seminar, companies use these analytic scoring products to predict, for example, the likelihood that a certain transaction will result in fraud, the credit risk associated with certain mortgage loan applications, whether sending a catalog to a certain address will result in an in-store or online purchase, and, in some cases, what prices to charge to consumers. While some speakers at the seminar pointed to the benefits of these predictions, such as providing the personalization that many consumers want and reducing costs associated with fraud,<sup>21</sup> others raised concerns about the potentially unregulated use of these tools in ways that mimic data uses regulated by laws such as the Fair Credit Reporting Act (“FCRA”) or the Equal Credit Opportunity Act.<sup>22</sup>

For example, if a company buys my credit score from a third party and uses it to deny me credit, I would be entitled to the full protections provided by the FCRA. Such protections include an adverse action notice, which informs me that a consumer report was in the denial and enables me to request the report and dispute any inaccuracies in it. On the other hand, if the company uses its own in-house Big Data analytics to generate a score, I may not be entitled to these protections. As another example, while traditional credit scores use factors drawn from an individual’s credit report, other aggregate or modeled credit scores draw on the data of a group of individuals, and thus may fall outside of the protections of federal law. In other words, if a company lowers my credit limit based on a score that reflects my own credit history, I would be entitled to full protections under the FCRA. If, however, the same company lowers my credit limit based on the scores of a group in which I am a member, the application of the FCRA may be less clear. These practices could negatively affect certain populations, such as low-income or minority consumers, by limiting their access to credit.<sup>23</sup>

Speakers at our seminar also raised concerns about the use of Big Data to engage in price discrimination. While some stated that competition could resolve consumer concerns regarding dynamic pricing,<sup>24</sup> others expressed concern that consumers in lower-income neighborhoods without competition from brick-and-mortar stores would be charged higher prices.<sup>25</sup> We intend to explore these issues further at our September 15 workshop on Big Data.

---

<sup>21</sup> See, e.g., Alternative Scoring Products Seminar, Mar. 19, 2014, Tr. at 22-38, available at [http://www.ftc.gov/system/files/documents/public\\_events/182261/alternative-scoring-products\\_final-transcript.pdf](http://www.ftc.gov/system/files/documents/public_events/182261/alternative-scoring-products_final-transcript.pdf)

<sup>22</sup> See, e.g., *id.* at 38-43.

<sup>23</sup> See, e.g., *id.* at 54-55.

<sup>24</sup> See, e.g., *id.* at 69-72.

<sup>25</sup> See, e.g., *id.* at 62-64, 75-76



## C. RESPONSES TO SPECIFIC QUESTIONS

The NTIA Request for Comment posed a number of questions, including questions about possible approaches for addressing the privacy risks of Big Data. This comment addresses three such approaches: (1) de-identification of data (2) accountability mechanisms, and (3) notice and choice for consumers. As discussed below, all three of these approaches remain important tools for protecting privacy in the era of Big Data.<sup>26</sup>

### 1. De-identification

As discussed in the FTC's Privacy Report, technological advances and Big Data analytics allow companies to combine disparate pieces of data to identify a specific consumer, computer, or device, even if the individual pieces of data do not themselves constitute personally identifiable information ("PII"), such as name and contact information. Not only is it *possible* to re-identify non-PII data through various means, but businesses have strong incentives to do so. As a result, the Commission has stated that privacy protections should apply, not only to traditional PII, but also to data that, while not yet linked to a particular consumer, computer, or device, may reasonably become so.<sup>27</sup>

The FTC Privacy Report set forth three steps that a company should take if it wants to ensure that data is not reasonably linkable to a consumer, computer or device. First, the company should take reasonable measures to ensure that the data is de-identified. Second, it should publicly commit to maintain and use the data in a de-identified fashion, and not to attempt to re-identify the data. And third, if the company makes such de-identified data available to other companies – whether service providers or other third parties – it should require such entities to commit that they will not re-identify the data.

This three-part test recognizes that, as technology continues to develop, there is always a possibility that a piece of data could be linked to a consumer, computer, or device. However, by cabining privacy protections to data that is not *reasonably* linkable to a particular consumer, computer, or device, this approach provides companies with an incentive to collect and use data in de-identified form, which reduces the privacy risks associated with that data. And by requiring companies to publicly commit to steps to assure that the data remains de-identified, this

---

<sup>26</sup> The FTC Privacy Report addressed these approaches in outlining a framework for businesses to protect consumer information. Likewise, the President's Consumer Privacy Bill of Rights, supported by the Commission, contained similar goals. See WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY [hereinafter CPBR] (Feb. 2012), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

<sup>27</sup> See PRIVACY REPORT, supra note 8, at 18-22.

approach promotes strong and continuing protections even as the collection, use, and sharing of Big Data continues to expand.

## 2. Improved Accountability

Accountability is a key component of privacy protection, and Privacy-by-Design is an important way to promote accountability. As noted above, “Privacy-by-Design” refers to the practice of promoting consumer privacy throughout a company’s organization and at every stage of the development of its products and services. In the era of Big Data, which may involve the collection, manipulation, and use of consumer data in multiple functions of an organization, Privacy-by-Design enables a company to promote accountability across all of these functions.

Privacy-by-Design includes incorporating substantive privacy protections such as data security, data accuracy and data minimization. It also includes the adoption of procedural protections, such as designating personnel responsible for employee privacy training and regularly assessing the privacy impact of specific practices, products, and services. By making commitments to treat data in a responsible manner, a company can provide basic privacy protections that are consistent with its business model and do not require consumers to read long and incomprehensible privacy notices to obtain them.

The Commission’s settlements with Google,<sup>28</sup> Facebook,<sup>29</sup> Myspace,<sup>30</sup> social networking app Path,<sup>31</sup> and Snapchat<sup>32</sup> illustrate how these principles can work in practice. In those cases, the Commission alleged that the companies deceived consumers about the level of privacy afforded to their data. The FTC’s orders require the companies to implement a comprehensive privacy program reasonably designed to address privacy risks related to the development and management of new and existing products and services. The privacy programs must, at a minimum, contain certain controls and procedures, including: (1) the designation of personnel responsible for the privacy program (2) a risk assessment that, at a minimum, addresses employee training and management and product design and development (3) the implementation of controls designed to address the risks identified (4) appropriate oversight of service providers, and (5) evaluation and adjustment of the program in light of regular testing and monitoring.

---

<sup>28</sup> Google, Inc., No. C-4336 (F.T.C. Oct. 24, 2011), available at <http://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter>.

<sup>29</sup> Facebook, Inc., No. C-4365 (F.T.C. Aug. 10, 2012), available at <http://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc>.

<sup>30</sup> Myspace, LLC, No. C-4369 (F.T.C. Sept. 11, 2012), available at <http://www.ftc.gov/enforcement/cases-proceedings/102-3058/myspace-llc-matter>.

<sup>31</sup> United States v. Path, Inc., No. CV13-00448-RS (N.D. Cal. Feb. 1, 2013), available at <http://www.ftc.gov/enforcement/cases-proceedings/122-3158/path-inc>.

<sup>32</sup> Snapchat, Inc., File No. 132 3078 (F.T.C. May 8, 2014), available at <http://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter>.

As these orders demonstrate, a key component of Privacy-by-Design is conducting a risk assessment to identify privacy risks and developing a program reasonably designed to address them. In the Big Data context, this should include considering privacy risks in designing algorithms and predictive analytics as applied to consumer data. Implementation of such a program can go a long way towards minimizing the risks associated with Big Data.

### **3. Notice and Choice**

The FTC Privacy Report and the White House Big Data Report both discuss the practical limitations of the traditional “notice and choice” model for addressing privacy, in which a company discloses its privacy practices in a lengthy privacy policy to which consumers are essentially deemed to have agreed. Among other things, data practices have become increasingly complicated and difficult to describe; privacy policies have become extremely long and impossible to understand; consumers are increasingly accessing the products and services on-the-go, using devices with small screens; and many companies that collect data are behind the scenes and entirely unknown to consumers. These concerns are exacerbated in a world of Big Data, where data collection is ubiquitous and constant. It is simply impossible to provide notice to consumers every time data is collected or shared.

To reduce burdens on both businesses and consumers, the Commission has recommended that companies communicate meaningful choices to consumers in simpler ways.<sup>33</sup> Accordingly, in the Privacy Report, the Commission explained that companies should not have to provide choices before collecting and using consumer data for practices that are consistent with the context of the transaction or the company’s relationship with the consumer.<sup>34</sup> Consumers expect these data uses, so neither consumers nor companies should be burdened to seek and obtain consent for them.<sup>35</sup> On the other hand, if a company’s data collection or use is not consistent with this context, the company should offer the choice at a “just in time” point, when the consumer is making a decision about his or her data, and not buried in a lengthy privacy policy.

In addition, certain data uses may be so sensitive, or contrary to consumer expectations, that they require more prominent notice and choice. For that reason, the Commission’s Privacy Report recommended that companies obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected, or (2)

---

<sup>33</sup> Of course, privacy policies continue to serve an important accountability function by providing the impetus for companies to evaluate their privacy practices and communicate these practices to the public.

<sup>34</sup> See PRIVACY REPORT, supra note 8, 35-60.

<sup>35</sup> This standard is consistent with the CPBR’s “Respect for Context” principle, which states: “Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.” CPBR, supra note 26, at 15. This principle is particularly important in the Big Data environment, when downstream uses of data often are not clear to consumers.

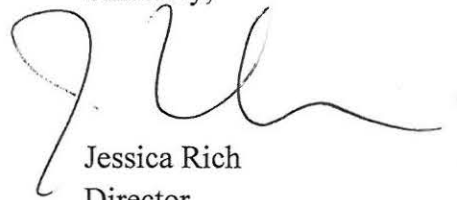
collecting sensitive data, such as information about children, financial and health information, Social Security numbers, and precise geolocation data.<sup>36</sup> This approach strikes an appropriate balance between consumer privacy interests and legitimate data use. It gives consumers control over the collection and use of their data, sets clear expectations for both consumers and businesses, decreases the burdens created by a “pure” notice and choice model, and preserves the ability of companies to use Big Data to innovate and improve products.

#### **D. CONCLUSION**

As discussed above, protecting consumer privacy remains a top FTC priority in the era of Big Data. Although changes in the marketplace have required adjustments to existing tools for protecting privacy, many of these tools – including those highlighted above – remain a critical part of an effective privacy program.

Thank you for this opportunity to respond to your Request for Comment.

Sincerely,

A handwritten signature in black ink, appearing to read 'J. Rich', with a long horizontal flourish extending to the right.

Jessica Rich  
Director  
Bureau of Consumer Protection

---

<sup>36</sup> See PRIVACY REPORT, *supra* note 8, at 57-60.