FTC Report "Data Brokers: A Call for Transparency and Accountability"

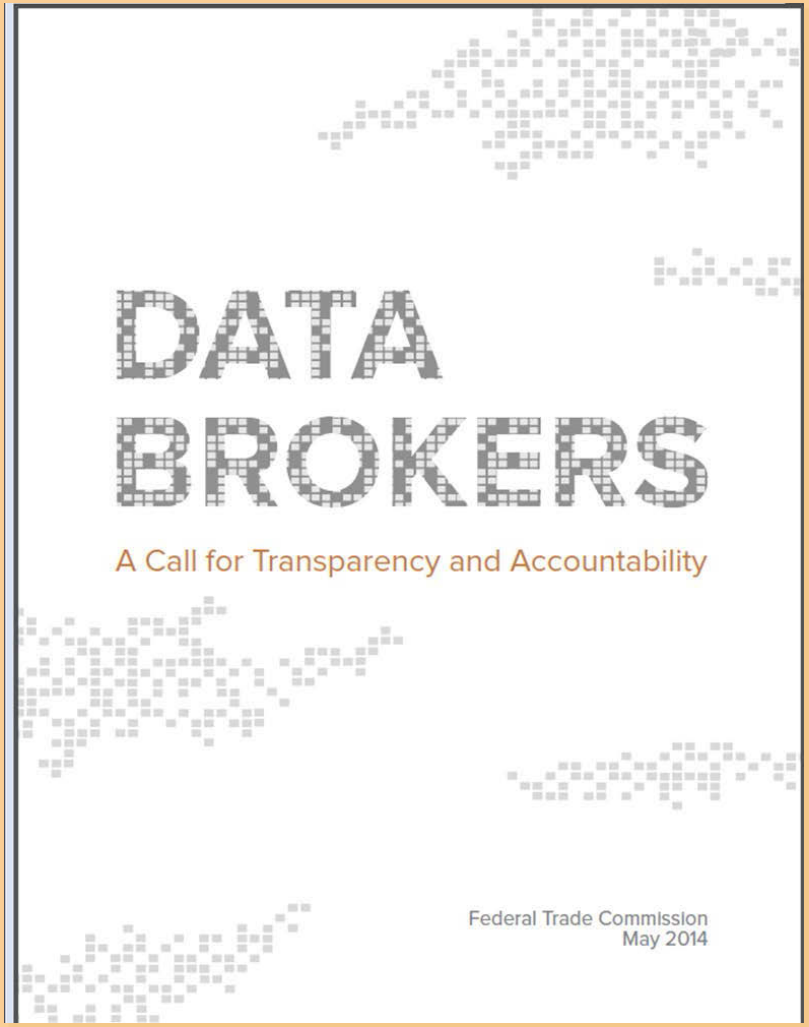
NCVHS Hearing on De-Identification and HIPAA
May 24, 2016

Cora Han, Attorney
Federal Trade Commission
Division of Privacy and Identity Protection

The views expressed are my own and not those of the FTC or any individual Commissioner.

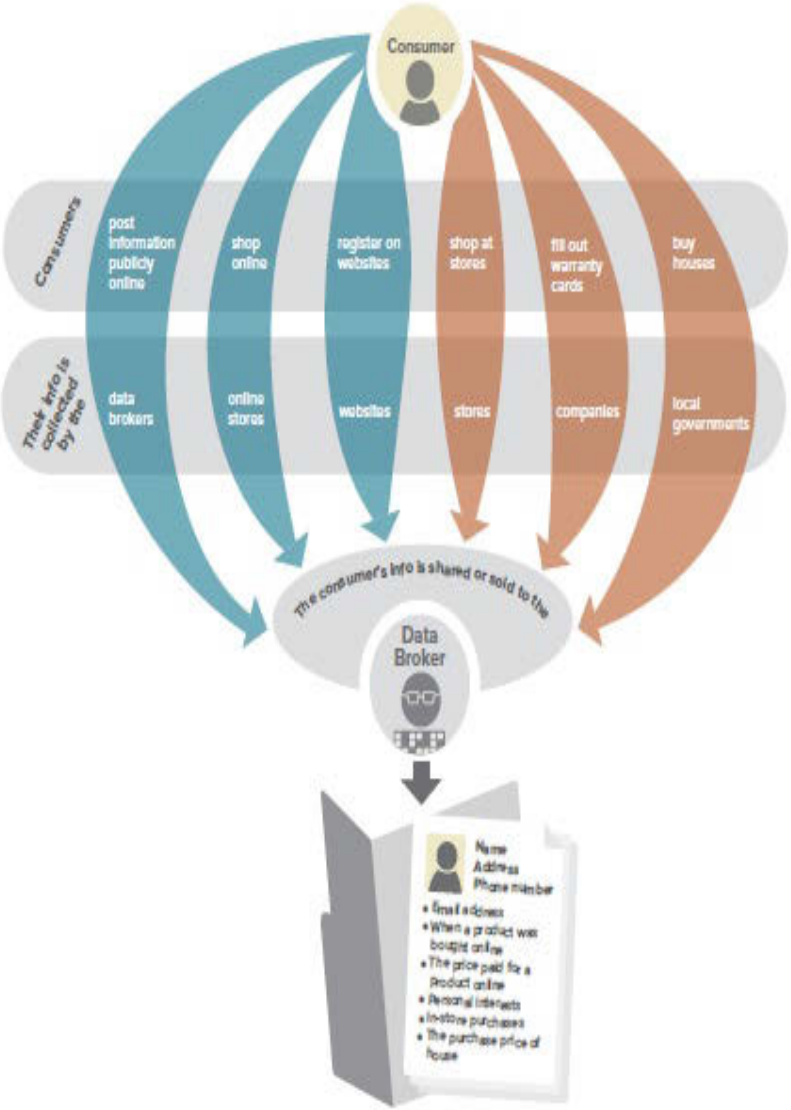
Data Broker Report

- Sent information requests to nine data brokers:
  - Nature and sources of data?
  - Use, maintenance, and dissemination of data?
  - Give consumers access, and the ability to correct and/or opt out?
- The report:
  - Summarizes findings
  - Proposes legislation
  - Recommends best practices



Data Collection
Online & Offline

As consumers go about their business, data brokers may collect information about them.



Data Broker Report

- Data Sources
  - Government
  - Publicly available sources
  - Commercial data sources
- Development of Products
  - Creation of data elements and segments
  - Data suppression
  - Data storage
- Types of Products
  - Marketing
  - Risk mitigation
  - People search

Data Broker Report Findings: Characteristics of the Industry

- Data brokers collect consumer data from numerous sources, largely without consumers' knowledge.
- The data broker industry is complex, with multiple layers of data brokers providing data to each other.
- Data brokers collect and store billions of data elements covering nearly every U.S. consumer.
- Data brokers combine and analyze data about consumers to make inferences about them, including potentially sensitive information.
- Data brokers combine online and offline data to market to consumers online.

Data Broker Report Findings: Consumer Choices

- To the extent data brokers offer consumers choices about their data, the choices are largely invisible and incomplete.
  - Marketing: Limited access and not all allow correction
  - Risk mitigation: Not all provide access and only one allows for correction
  - People search: Not all allow consumers to opt-out

Data Broker Report Findings: Benefits and Risks

- Consumers benefit from many of the purposes for which data brokers collect and use data.
  - Prevent fraud
  - Improve product offerings
  - Deliver tailored advertisements to consumers
- Many of the purposes for which data brokers collect and use data pose risks to consumers. Examples:
  - Inability to conclude a transaction based on an error in a risk mitigation product
  - "Biker Enthusiast" data segment could help a motorcycle dealership offer a consumer coupons, but it could also be used by an insurance company to assume the consumer engages in risky behavior
- Storing data about consumers indefinitely may create security risks.

Data Broker Report Recommendations

- Legislative
  - Notice and disclosure
  - Access and correction
  - Opt out and suppression
- Best Practices
  - Privacy by Design
    - Collect only data needed
    - Dispose of data as it becomes less useful
  - Refrain from collecting from children and teens
  - Ensure downstream users don't use information for FCRA or discriminatory purposes

Big Data Report

- Big Data: A Tool for Inclusion or Exclusion
  - September 2014 Workshop
  - Spring 2014 Seminar on Alternative Scoring Products
- The report
  - Life cycle
  - Benefits and risks
  - Potentially applicable laws
  - Recent research

De-identification

- Reasonable steps to de-identify data – including by keeping up with technological developments
- Public commitment not to re-identify
- Enforceable contracts, requiring any third parties to commit not to re-identify

Questions?
chan@ftc.gov

The Washington Post

Demanding transparency from data brokers

By Julie Brill, Published: August 15

Julie Brill is a member of the Federal Trade Commission.

Revelations about the extent to which the National Security Agency (NSA) collects personal information started a robust national debate on how best to balance national security and privacy rights. Last month, members of the House of Representatives questioned the funding for the government's data-collection programs, and last week the White House proposed steps to increase the transparency of those programs. Along the way, consumers have gotten a crash course in the price we pay to participate in the online and mobile marketplace: Our most intimate information floats free in cyberspace, ripe for any data miner — government or otherwise — to collect, use, package and sell.

All day long, as we surf the Web, tap at apps or power up our smartphones, we send digital information out into cyberspace. As we live our wired lives, we constantly add to the veins from which data miners pull pure gold. It took the NSA revelations to make concrete what this exchange means: that firms, governments or individuals, without our knowledge or consent, can amass large amounts of private information about people to use for purposes we don't expect or understand.

Many tech firms are calling on the government to allow them to reveal how and how often the government seeks information about individuals. We ought to demand the same sort of transparency from the commercial data brokers that know much more about us than we do about them. One of the largest, Acxiom, reportedly has information on about 700 million active consumers worldwide, with some 1,500 data points per person. Such data brokers learn about us from the cookies that hitch rides as users travel online and from the social media sites where we post everything from home addresses to pictures to magazine subscriptions and store purchases, as well as deeds on file in towns and counties. They load all this data into sophisticated algorithms that spew out alarmingly personal predictions about our health, financial status, interests, sexual orientation, religious beliefs, politics and habits.

These dossiers are the reason that when I log in, I see an ad for suede boots but my son sees the release date for the latest "Call of Duty" game. This may seem benign, but increasingly our data fuel more than just what ads we are served. They may also determine what offers we receive, what rates we pay, even what jobs we get.

The Fair Credit Reporting Act (FCRA) provides some protections. The law requires that entities that collect information for those making employment, credit, insurance and housing decisions do so in a manner that ensures the information is accurate. The Federal Trade Commission targets firms that screen potential tenants, credit recipients, employees and insurance purchasers without complying with the law. But in an online world in which companies large and small innovate constantly and — sometimes unknowingly — push legal boundaries, it is difficult to reach all of those who may engage in activities that fall afoul of the FCRA.

Further, personal data could be — and probably are — used by firms making decisions that aren't regulated by the FCRA but still affect users' lives profoundly. These include determinations about whether we are too risky to do business with or aren't right for certain clubs, dating services, schools or other programs. Citizens don't know what of our personal information is on file or how it is being used, and this frames the fundamental challenge to consumer privacy in the online marketplace: our loss of control over our most private and sensitive information.

Changing the law would help. But even without legislation, we can begin to address the problem with a comprehensive initiative to give consumers the knowledge and tools they need to reassert some control over their personal data.

This approach, which I call Reclaim Your Name, can be adopted by the industry without a government directive. Its four basic components would empower people to find out how brokers are collecting and using their data; give people access to information that data brokers have amassed about them; allow people to opt out if they learn that a data broker is selling their information for marketing purposes; and provide consumers the opportunity to correct errors in information used for decisions about substantive benefits.

More than a year ago, I called on the data-broker industry to develop a user-friendly, one-stop online shop to achieve these goals. In a helpful move, the chief executive of Acxiom, Scott E. Howe, recently announced plans to open his company's dossiers to consumers. I invite Howe, his compatriots Bryan Kennedy at Epsilon and Don Robert of Experian, and other industry leaders to come to the table and hash out how we can put the principles of Reclaim Your Name into practice.

There is no reason that data brokers and firms that use consumer data cannot coexist with a system that empowers consumers to make real choices about how our privacy information is used. Such a system would go a long way toward restoring consumer trust in the online and mobile ecosystems, allowing us to continue to enjoy all the convenience, entertainment and wonder that cyberspace has to offer.

Read more about this issue: Jon Leibowitz: Protecting privacy in a TMI world Michael Chertoff: Cloud computing and the looming global privacy battle The Post's View: Google's privacy policy complicates the protection of personal data Outlook: Five myths about privacy The Post's View: In NSA programs, democracy works in secret