Losing the Privacy War - Data Aggregation

Dr. Margaret Leary, CIPP/G, CISSP, CRISC, CE|H

Data Aggregation

- Brokers collect large amounts of data on citizens, through scribes at court house public records, or by purchasing data from affiliates (partners).
- Collection is not transparent, most citizens are unaware that the data is being collected on them.
- FTC found that broker relationships are complex, often selling or ***exchanging data with other brokers***.
- Often, brokers develop their own scoring algorithms that just provide a "score" to the service consumer, based on proprietary analytics.

"Of the nine data brokers, one data broker's database has information on 1.4 billion consumer transactions and over 700 billion aggregated data elements; another data broker's database covers one trillion dollars in consumer transactions; and yet another data broker adds three billion new records each month to its databases."

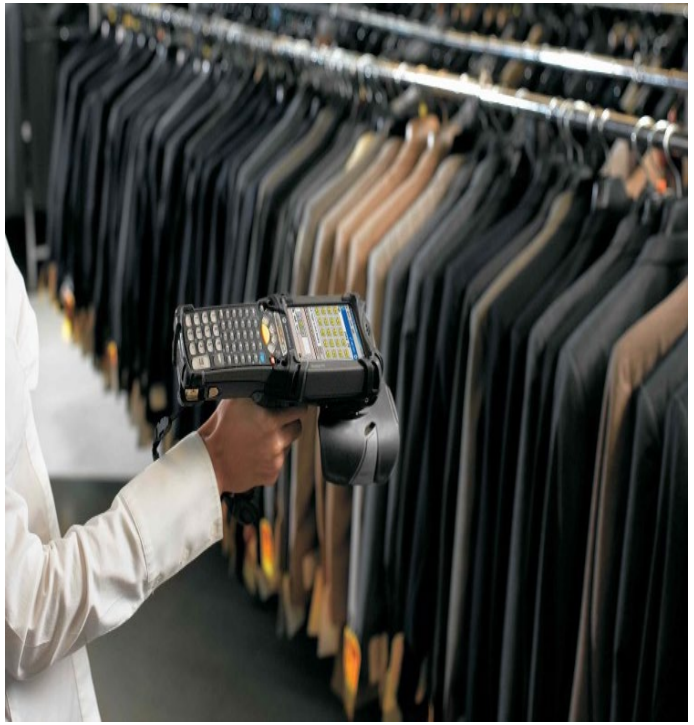
FTC Report "Data Brokers: A Call for Transparency and Accountability"

It is estimated there is more than 1.7 mb of data collected on every individual on the planet – every second.

Who Collects/Sells Your Data?

- When surveyed, companies state that your data is their most valuable asset!
- Banks and credit card companies
- Hospitals
- Federal and State agencies provide data
- Retail store owners who sell sales records
- Smart TVs, phones, and watches
- Utility companies
- Warranty Registrations
- Location data with Fitbits and other devices
- Barbies (Hello Barbie)
- Tik Tok!!!!
- Your clothes (formerly “spychips”, now inventory tags)
- RFID Chips in people?

Flat Orb advertises that it tracks your product AND your staff



Problem with Opt-Out to Data Sharing

CHASE

Rev. October 2014

FACTS	WHAT DOES CHASE DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ▪ Social Security number and income ▪ account balances and transaction history ▪ credit history and payment history
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Chase chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Chase share?	Can you limit this sharing?
For our everyday business purposes – such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes – to offer our products and services to you	Yes	No
For joint marketing with other financial companies	Yes	No
For our affiliates' everyday business purposes – information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes – information about your creditworthiness	Yes	Yes
For our affiliates to market to you	Yes	Yes
For nonaffiliates to market to you	Yes	Yes

PLS11076 10/1/2014

PNC10698 FEDPRIV

INS16086 CAF15-PRIV

You Get What You Pay For Google

*"**All users of email must necessarily expect that their emails will be subject to automated processing.** Just as a sender of a letter to a business colleague cannot be surprised that the recipient's assistant opens the letter, people who use web-based email today cannot be surprised if their emails are processed by the recipient's [email provider] in the course of delivery. Indeed, **"a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."***

Google Court Filing August 2013 - Mick, Jason, 2013. "Google: Yes, we "Read" Your Gmail"

- **Feeling glad that you aren't one of the 425 million Gmail users? Don't be – have you sent an email to a Gmail user?**

- Facebook’s Terms of Use specifies that, while you “own” all content and information you post, you grant them a nonexclusive, transferable, sub-licensable, **worldwide** license to use all IP content that you post on or in connection with Facebook.
- U.S. courts have confirmed that if the data is voluntarily shared with another then it can be posted publicly.
- Even privatized information on Facebook is collected and sold by Facebook to their business partners and to Federal Agencies

Government as a Consumer of Aggregated Data

- Used for direct marketing, marketing analytics, identify verification, fraud detection, people search. Specific examples include:
  - Used for criminal investigations or who may commit a crime (threats on social media)
  - Security clearances
  - Identity authentication
  - Employment considerations
- Predictive analytics:
  - Fraud predictions: scoring individuals based on public and private databases and social media, based on their “risk for fraud”, negatively impacting nursing home residents waiting for Social Security, Medicaid, Children’s Health Insurance Programs, Supplemental Nutrition Assistance programs, and other Federal or State government benefits.

Data Aggregation's Impact on Citizens

- Impose marketplace disparities on gender and POC (Consumer Federation of America) as they "categorize" by gender, ethnicity, and income levels
- Impose auto insurance surcharges on blue-collar workers and those without college degrees (Consumer Reports)
- Impose higher health insurance rates if social media isn't consistent with desired lifestyle
- Impact ability to rent an apartment
- Impact employability

STATE REGULATION

Oregon Women Charged $100 More Than Men for Basic Auto Insurance; Drivers with Poor Credit Scores See Rates Double, According to New Research

Consumer Group Calls on Oregon Legislature to Reform Auto Insurance Rates, Help Safe Drivers

February 24, 2021 | Press Release

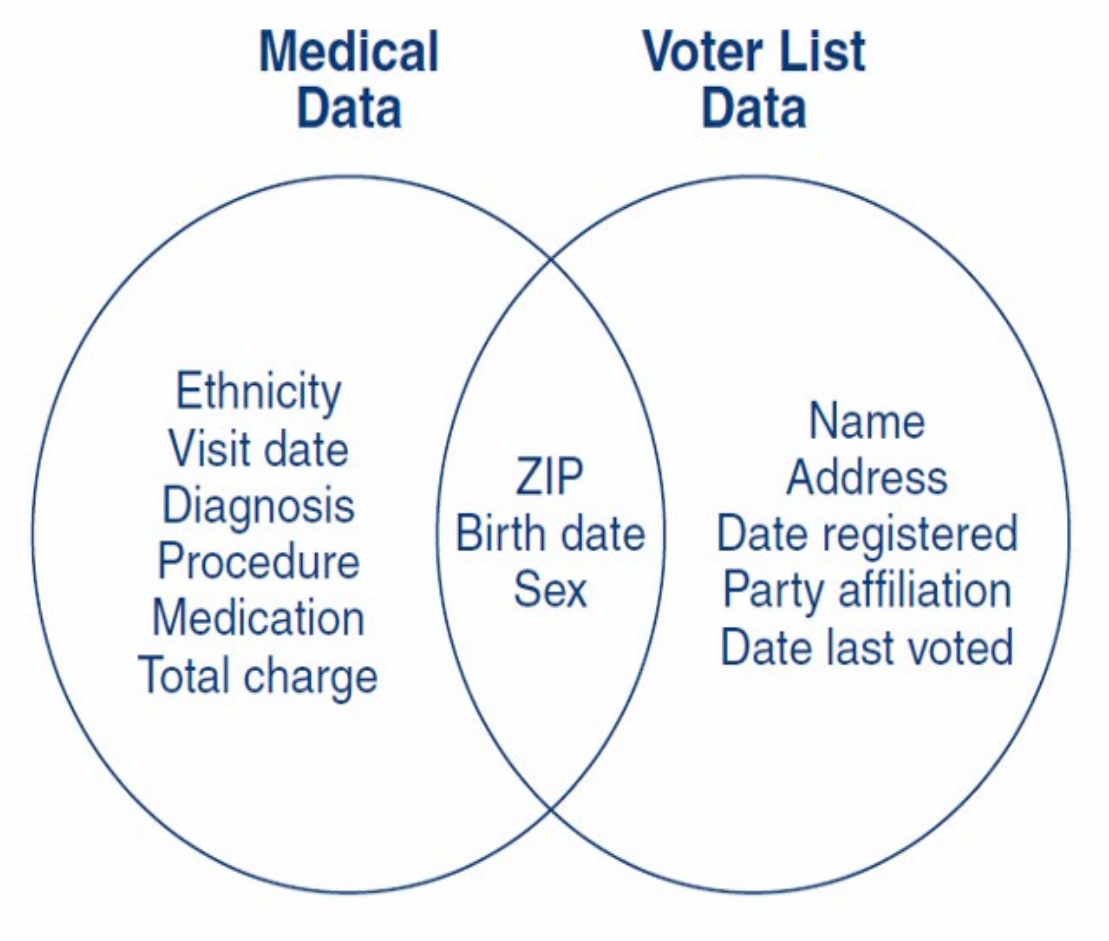
Consumer Federation of America at https://consumerfed.org

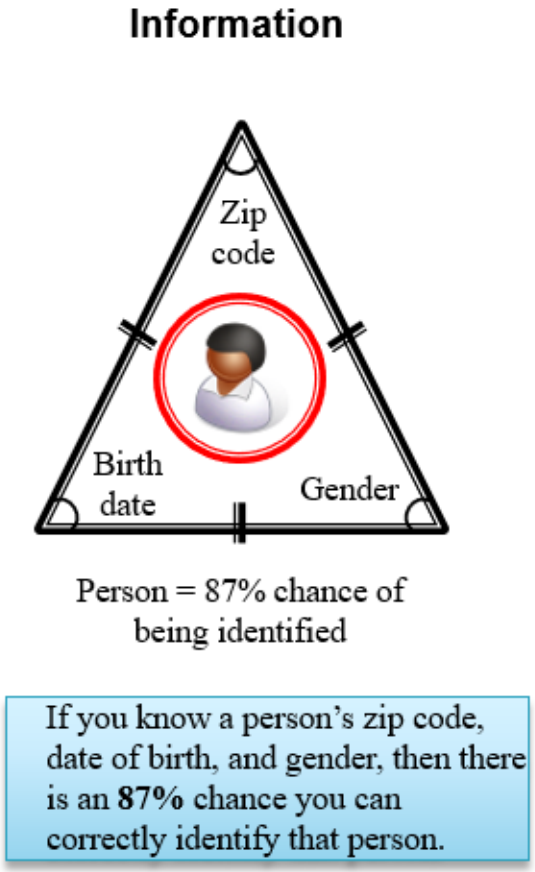
Conduit to Identity Theft if Not Secured?

- At stake is a data aggregation industry worth half a billion dollars.
- Collected data is used to calculate FICO scores and insurance rates, as well as form security questions for authenticating individuals to sensitive applications (financial services) include:
  - Favorite teacher?
  - SSN
  - DOB
  - Name of first pet?
  - Who holds your mortgage?
  - For how much did you finance your car?
  - Square footage of your house?
  - Mothers maiden name
- Service providers (Acxiom, Corelogic, ID Analytics, Equifax, LexisNexus, Experian, Pondera, etc.) provide KBA services to all businesses, state, and federal agencies, including to VitalCheck for Birth Certs (“Breeder Docs”)

***Identity attributes in red are those that were lost in the Equifax breach**

The Problem with Aggregation





Latanya Sweeney, k-anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10 (5), 2002; 557-570.

Recommendations

- Legislation must allow for transparency so that the consumer can identify who is collecting and sharing data, and for what purpose the information is shared.
- Congress needs to enact legislation to prevent Federal agencies from circumventing the Privacy Act by procuring broker services by establishing SORNs and PIAs for these services as they do for data they collect.
- Remove VCDPA exemptions for businesses who are not “selling” data, but “only” exchanging data with affiliates.
- Remove VCDPA exemptions for financial institutions and healthcare entities
- If a Federal Privacy Bill is enacted, it should be modelled on EU Opt-In policies, vice Opt-Out policies.
- Services, such as insurance or fraud services, that use broker data for risk mitigation, need to specify this **clearly** on their sites.
- Establish minimum security standards