CFPB Request for Comments on Data Brokers, 2023

Submitted:
July 14, 2023

Comments By:
Heidi Saas, JD, CIPP/US
Licensed in CT, MD, & NY
H.T. Saas, LLC

What happened to the truth? Do we even know how to find it anymore? How did we get into this digital mess? How can we get our personal information rights back? Thank you CFPB for trying to answer these difficult, yet critical questions, and for this opportunity to submit comments. Please return personal data rights to consumers, and regulate data brokers as credit reporting agencies. Resellers suck, and they will either get in line with the new rules, or they should cease to exist.

Privacy is a human right. Our Constitution does not include the word "privacy" but it remains fundamental to our "pursuits of happiness" and has deep roots in our nation's history. Privacy is essential to our identity, as individuals, and as a country. The rights of privacy we are currently relying upon, lie primarily within the 4th and 14th Amendments. Our friends in the EU have created rights belonging to the individuals (data subjects) and their GDPR rules give them enforceable rights and agency over the use of their data. In the US, we have tried to resolve the issue by placing obligations on businesses, when we should have been focused on securing the rights of individuals and establishing rules for businesses to follow to ensure those rights are respected.

The Fair Credit Reporting Act was enacted in 1970 to give consumers rights over the data used in credit reports. At that time, these reports were the only source of information about individuals. In 2003, FACTA was passed, amending the FCRA and excluding "resellers" from compliance with the obligations under the FCRA. This was the beginning of the data broker economy. Since that time, consumers have had no control over their data: how it was used, collected, sold, shared, processed, or used against them when applying for a job, a loan, or housing. These decisions, and how they are made, are regulated by various laws, but they are not being enforced because people do not understand how artificial intelligence and autonomous systems work with our data. Adverse action notices are not being sent,

and consumers have no way to discover what information is being used in these life-critical decision making processes.

We allowed for innovation for the past 20 years (at the expense of consumers), and now that we can clearly see the harms being created, we need to take remedial action to prevent future harms, and balance the legitimate data needs of businesses with the privacy rights of consumers. Please repeal the reseller exception. Everyone in the supply chain of our data should be held to the same standards for privacy and security. No exceptions, including non-profits and the government.

Data broker collect unverified data and put into personal profiles about us, they make inferences about us using this garbage data, and they sell it with reckless abandon. The chart below shows the types and amounts of information you can get from a credit report vs a profile. I made the chart, but feel free to use it.

Credit Reports, regulated by the Fair Credit Reporting Act (FCRA), allegedly used for employment, housing, lending, and insurance.	**Un-Regulated "Personal Profiles"- digital exhaust, scraped online records, and AI generated behavioral inferences, specially designed for targeted advertising purposes. Used for employment, housing, lending, insurance, stalking, and as a 4th amendment loophole for law enforcement.**
A list of businesses that have given you credit or loans	names, addresses, telephone numbers, e-mail addresses, gender, age, marital status, children, education, profession, income, political preferences, and cars and real estate owned
The total amount for each loan or credit limit for each credit card	bank account balances, amount of debt load for each credit card, data on an individual's purchases, where they shop, and how they pay for their purchases
How often you paid your credit or loans on time, and the amount you paid	geo location data
Any missed or late payments as well as bad debts	health information
A list of businesses that have obtained your report within a certain time period	the sites we visit online, the videos we watch, our DM messages
Your current and former names, address(es) and/or employers	the advertisements we click on
Any bankruptcies or other public record information	Not facts, but inferences made up about us: sexual preferences, reproductive health, gambling and other addictions, eating disorders, political views, religious views, family and friend associations, hobbies, fitness routines, suggested salary, whistleblower risk, and more.

Privacy concerns after the Dobbs decision have been accelerated into SAFETY concerns for women. State laws are changing rapidly, and the Supreme Court is unraveling the fabric of our society, in the name of their god. This is not justice, and it is destroying the essential freedoms of our democracy. No one wants to be hunted, and it is disgusting that the state of Texas pays cash bounties to hunt down women seeking health care. All health data should be treated as sensitive, whether collected through an app, or a DM conversation with your doctor. HIPPA came before apps, and those intended protections remain inadequate and must be updated in a more permanent way than Executive Orders. Data brokers should not be allowed to broker in such sensitive data. We cannot keep going down this road.

Privacy was a safety issue before Dobbs. Domestic violence issues often involve stalking and harassment, in addition to financial crimes and physical violence. Geo-specific location data is readily available, cheap, and easy for anyone to buy. Saying that data has been "aggregated" does not remove the possibility of re-identification, which has been demonstrated to be quite easy to accomplish. If we require technical measures to ensure privacy is achieved through the use of privacy enhancing technologies, such as differential privacy, we need to make sure they work. We need to require de-anonymization attacks, just like we require penetration testing for cyber security. Verification is essential to ensure the protection of our data, and our rights.
https://www.nature.com/articles/s41467-021-27566-0
https://leakuidatorplusteam.github.io/preprint.pdf

Economic harms are also being done in the areas of employment, housing, lending, and education. The collection, processing, and use of unverified and scraped data is the direct cause of "false light" profiles being used against consumers. Garbage data, categorized into clever segments for targeting, and sold indiscriminately for use by businesses all but renders the credit reports useless. Why would a business pay extra to comply with the FCRA obligations if they can just buy the data as "insights" to conduct their business, and the skirt regulations? Targeted marketing for jobs leaves workers looking to move up in their careers, faced with options at or below what the AI tools says they will accept. How do you apply to a job that is never marketed to you? The use of these tools has not improved the employer/ employee relationship as evidenced by the "great resignation". If the job match was so perfect for the candidate, why would they quit so often, with such animosity, and in such large numbers. Researchers at Harvard found that 80% of hiring managers know these tools screen out large numbers of qualified candidates.

This system does not work for businesses, or consumers, and the EEOC is overwhelmed by the cases before them related to these issues. The backlog for investigations is currently between 12-18 months. Consumers cannot just wait for justice when they need to work, right now. We have automated structural racism by integrating these craptech tools into our systems, and discrimination continues to widen the gaps in income disparity. Cycles of poverty cannot be broken if the machines determine your fate for you. Bias is real, and continuous audits (and remediation) must be required for all AI tools used in life-critical decision making processes. I worked with ForHumanity on drafting the criteria for how to conduct an audit for bias in artificial intelligence, AI, and autonomous tools, and we are currently expanding it to cover the EU's AI Act. Data broker's inferencing tools must be audited and monitored for harms to humans.
https://forhumanity.center/nyc-bias-audit/

The lack of regulations and oversight of the data broker industry has also created harms to businesses, especially small businesses. Anti-competitive behavior by the large platforms continues, and businesses are left without alternatives to these mammoth service providers. Their business data is shared, analyzed, packaged, and sold without the consent of the business owners, who lack any sort of leverage in these contract negotiations. "Dynamic pricing" may be a term of their agreement, but when the business owner asks to verify how the tool works to determine these "dynamic prices" the platforms push back hard with "proprietary and confidential information" as their reason for denying access, transparency, and accountability. How are businesses supposed to compete on a level playing field, if all of their business information is known by their competitors and used against them?

Ad fraud is also a raging dumpster fire that no one is watching. It is the root cause of waste in the digital economy. It is difficult to find, and may happen 3 or 4 times removed from the original marketer's campaign. The Real Time Bidding (RTB) process is a massive, ongoing data breach, and programmatic advertising must be cleaned up. Behavioral tracking must be banned. "Data hygiene" is a marketing term intended to shift liability to consumers, for the acts of data brokers, and I reject this rouse. Consumers did not create this problem. The data brokers dumped all of their cookies, pixels and other trackers into our devices, and they must be stopped from creating further harms. There are tools available to expose adfraud, and I encourage you to use this tool in your investigations. This tool was created by Dr. Augustine Fou, and it has been very useful to me and my colleagues in the privacy field for exposing ad fraud and data leakage. https://pagexray.fouanalytics.com/

Meta and Google Analytics cases have been litigated heavily in the EU, and they are not the only platforms mistreating our data in this manner. Pixels, beacons, cookies, and trackers are everywhere, including new types with injectable code, obscured behind tags with pixels. As soon as we identify a leakage issue, the platforms create another way to access the data, and keep going. These are unwarranted data breaches, perpetrated by the platforms to serve their own interests, not the businesses to which they were hired to provide a service. Businesses did not expect to hire them for surveillance as a service, endangering their business reputations and profitability. Research report from Adalytics on Google's Trueview:
https://adalytics.io/blog/invalid-google-video-partner-trueview-ads

Deletion of data is almost impossible, because our systems and tools were designed to collect and use data, indefinitely. Mandating data minimization is necessary, for our privacy, and for our environment. Space trash is a thing, and we are running out of room in the skies above Earth. The carbon footprint of the digital economy is enormous, and we cannot crash all of the useless satellites into the moon, nor run people out of the countryside with the environmental blight of the expansive data centers. We need to reduce the amount of data we use, to reduce the damage we are causing to the planet, and the harms to humans. If businesses were serious about their ESG goals, they would put data minimization under E, privacy respecting rules under P, and regulatory compliance under G. Consider a use case of a data deletion request from a former employee, who had administrator access. Everything they touched in the system became part of the infrastructure, and is necessary to the functionality of the system as a whole. Who has the rights here? The business, the employee, neither? Employee data rights need more protection and clarity, for both employees and businesses.

The FCRA is not a perfect law, but it could improve our digital futures, if our rights to our personal information were returned to us. Please repeal the reseller exception, and regulate all data brokers as credit reporting agencies under the FCRA.

Good luck, and thank you all!

Best wishes,

Heidi Saas