THE MARKET FOR PERSONALLY IDENTIFYING INFORMATION

November 2013

Cara Bloom

ABSTRACT

American citizens are constantly exchanging their personally identifying information for marginal benefits such as store discounts. It has been proven in behavioral economics research that consumers do not understand the value of their information, can easily be manipulated in to relinquishing it, and don't know what happens to that information once it has been given. Right to know legislation would require data aggregators to be more transparent about data collection and use, but they have been stopped by tough lobbying at the state and federal level. Data aggregator Acxiom has implemented a policy of transparency, leading the field and hoping to have a say in future legislation. Transparency such as this diminishes consumer surplus and makes the market for information more efficient.

INTRODUCTION

During the spring graduation season, families head to the local party store for all of their cards, balloons, and other party supplies. Customers who spend upwards of a hundred dollars on their party goods, as they often do, are offered a fifteen percent discount in return for their name and email address. I asked the store clerk how many people turn down the offer, her response: none yet.

There is an economy that many consumers do not know exists surrounding their own personal data. It's so easy to write down a name, email address, home address, or birthday that customers will often trade their personally identifying data for marginal incentives, not understanding the how much data brokers have on them, its use, or the value companies put on that information.

Privacy and consumer advocates lobby for more protective legislation, especially through corporate transparency, while large data aggregators fight to keep the current policy of leniency with allowances like opt out and the ability to sell data to third parties without notifying the data subject. Because individuals are often ignorant of the economic value of their data, large collectors of this information control the data markets, relying on the ease of acquiring enough data to run statistically significant – and extremely profitable – analysis. With increased awareness through legislation requiring transparency, the markets will shift towards the supplier (individual people who create data) and a more balanced market.

THE COMMERCIAL PRIVACY BILL OF RIGHTS

McCain and Kerry proposed this bill in 2011 to establish Fair Information Practice Principles for data collectors. The core tenants of the legislation were that companies must inform consumers what they are doing with the information, hold the data only until the defined goals are accomplished, and offer an opt-out from sharing with third parties. The policy encourages commercial groups to design products with privacy in mind from the start and to work with Federal Trade Commission. The proposal gave the law teeth as an additional encouragement: the FTC would have the power to impose up to six million in fines.[1]

Though this bill was not ratified by congress, it has been used in the framework of

[1] Harris, Leslie. "Do We Need a Privacy 'Bill of Rights'? Senate Considers One." *ABC News*. ABC News

subsequent proposals, most recently a framework created in response to Europe's growing concerns of US privacy policy. The new bill, similar to the Kerry-McCain bill, would create industry codes for the use of consumer data. Though this bill would assist the US's negotiations with Europe – especially in light of the Snowden revelations – large data brokers continue to cause delays.

Internet Association president Michael Beckerman stated,

> "We continue to favor industry self-regulation and agreements between Internet companies and their users as they are proven methods for safeguarding users' privacy while maintaining flexibility for continued creativity and innovation online."

Politicians have called the issue "complex and delicate" to explain their avoidance of regulatory action.[2]

"PRIVACY IS DELAYED GRATIFICATION"

Carnegie Mellon behavioral economist Alessandro Acquisti studied the delayed gratification of giving up personal data for immediate rewards in a recent experiment not dissimilar to the party store scenario. The question that guides his research is: "Do Americans value their privacy?"

In an experiment at Carnegie Mellon University, graduate students offered shoppers in a suburban mall a ten-dollar discount card for free, then an extra two-dollar discount in return for their shopping data. In other cases they offered shoppers a twelve-dollar card first, then told them they could only receive a ten-dollar card if they didn't want to share their data. While half of shoppers declined the first offer of an extra two-dollar discount, ninety percent of shoppers chose the twelve-dollar card in the second experimental group.

Shoppers were offered a $12 discount card and the option of trading it in for a $10 card to keep their shopping record private. Ninety percent chose to trade privacy for $2.

Acquisti concluded that context matters: shoppers who perceived that they

[2] Byers, Alex. "White House Pursues Online Privacy Bill amid NSA Efforts." *POLITICO*. N.p., 07 Oct. 2013. Web. 09 Nov. 2013.

"owned" the greater discount at the outset were more likely to value it, while shoppers who did not seem to have it would not give up information to acquire it. Economists would like to believe that consumers are rational, but this experiment demonstrations an irrational disparity in consumer valuations of their privacy by context.[3]

The inability to value information correctly suggests inefficiency in the market. Data brokers know exactly what the value a shopper's information is to the company, but the people do not know this evaluation, causing them to either value their data too high or more often too low. When the shopper trades information for less than the reserve price the data broker has placed on it, there is a consumer (data broker) surplus equal to the difference between the shopper and broker values for the data. Consumer surplus is inefficient, but if the two sides were to value the information equally – or if the consumer knew how much his or her data is worth – the inefficiency would be mitigated and equilibrium could be achieved.

When the data collector hid their reserve price for the information, almost all consumers were willing to part with their shopping data creating the consumer surplus. Shoppers did not know what the data would be used for or where it would go, but parted with it to keep the extra two dollars they had been offered. Under the Kerry-McCain bill these people would have been given much more information and an opt-out from third parties that would have shifted the market towards balance and efficiency.

RIGHT TO KNOW

Data collectors fear that right to know provisions like educating shoppers about how their purchase data is used and being required to give consumers their data when requested will handicap the industry, make them vulnerable to lawsuits, diminish their surplus, and even limit their ability to innovate. In response to the solution of giving data subjects the right to request their individual profile from a company, American corporations argue they would have to hire whole teams of new, expensive employees to handle the requests.

American corporations are no doubt looking to their European counterparts – and home-grown companies like Facebook – that have had to adapt to new EU right to know laws by spending millions of dollars on reworks. A coalition lawyer

[3] Sengupta, Somini. "Letting Down Our Guard With Web Privacy." *The New York Times*. The New York TImes Company, 30 Mar. 2013. Web. 10 Nov. 2013.

representing companies including Amazon, Facebook, and Verizon said that right to know was "not workable" because of its broad range.[4]

By implementing more restrictive privacy laws, the governments – whether they are international, national, or state bodies – are creating new costs for businesses. There are direct costs like those business incur when refitting their information models to comply with new laws, and indirect like the predicted increase in consumer data costs.

The indirect costs are often more worrisome because they are difficult to be calculated predictively. These costs include loss of customers dissatisfied with treatment or collection of their data who either work to protect their information or boycott the store, either way limiting the data they share and causing the price of data to rise.

When consumers describe business practices as "Orwellian," as was said after the Target pregnancy scandal, there is often a change in both consumer sentiment and practices. The pregnancy coupons incident went viral on media outlets across the country, causing a noticeable impact on the company.[5] Facebook has received similar backlash when issues with their privacy policy have gone viral.

While firms are hesitant to lose customers' purchases or information through backlash against their data policy, privacy advocates argue that this transparency is a right of the consumer. With tracking cookies or other methods, data brokers acquire data without the knowledge – and therefore without permission – of the person. In these cases, where consumers willingly trade information for marginal benefits, companies have the explicit permission because consumers have "opted in" to the agreement. Often there is fine print or Terms and Conditions that few people read with the specifics of the deal in legal jargon. People who agree to these terms and hand over information willingly often know just as little as those who are unknowingly tracked by cookies.[6]

---

[4] Sengupta, Somini. "No U.S. Action, So States Move on Privacy Law." *New York Times*. The New York TImes Company, 30 Oct. 2013. Web. 11 Nov. 2013.
[5] Moylan, Martin. *Target's Deep Customer Data Mining Raises Eyebrows*. Minnesota, 7 Mar. 2012. *MPR News*. Minnesota Public Radio, 7 Mar. 2012. Web. 11 Nov. 2013.
[6] "Big Brother Is Watching: Databases Collect Your Personal Information and Invasion of Privacy." *Consumer Reports Money Advisor* (2009): n. pag. *Consumer Reports*. Consumers Union of the US, Sept. 2009. Web. 12 Nov. 2013.

A recent PEW study has shown that a majority of Internet users value their privacy enough to "mask their digital footprints." Almost 70% of users do not think that current US privacy law is sufficient.[7] America is a democracy, governed for the people, by the people, so when more than two out of three Americans want a change, it is the government's obligation to create a logical legislative adjustment that fulfills the needs of its constituency. The right to privacy is not explicitly defined in the bill of rights, but it is being defined federally and on the state level. The Code of Fair Information Practices creates a baseline with principles that support right to know practices.[8] California has passed some of the most protective privacy bills, many of which coincide with the Code of Fair Information Practices, though their right to know bill was stopped by tough lobbying.

Some companies recognize users' growing focus on privacy. They either strengthen their privacy policy or offer incentives to mitigate consumers concerns. Few have opened up their databases for consumers to see what information a database has, how accurate it is, correct that data, or remove it all together. Surprisingly, the "big daddy of all data brokers" Acxiom has done just that.

ACXIOM

Based on consumer sentiments and an FTC report that recommends congress pass a law requiring data transparency from aggregators, Acxiom foresees regulation for data brokers such as themselves. "You may be surprised to know that we are in favor of heightened industry regulation, but we want to make sure we have a voice in the process," said Scott Howe, CEO of Acxiom. This company has implemented a right to know stance without legislation to become a model for other companies and potential legislation to come. It enhances their image, gives them a voice in future proceedings, and has not injured the company significantly with its easily editable data or accessible opt-out button.[9]

If consumers had flocked to the site to remove their profiles or falsify their data Acxiom's business could have taken a severe hit, but even before the launch top executives were not worried as past consumer behavior shows only marginal opt-

---

[7] Rainie, Lee, Sarah Kiesler, Ruogu Kang, and Mary Madden. *Anonymity, Privacy, and Security Online*. Rep. N.p.: Pew Research Center, 2013. *Pew Internet and American Life Project*. Web. 11 Nov. 2013.

[8] Nissenbaum, Helen Fay. "Chapter 2: Knowing Us Better than We Know Ourselves: Massive and Deep Databases." *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law, 2010. N. pag. Print.

[9] Singer, Natasha. "A Data Broker Offers a Peek Behind the Curtain." *The New York Times*. The New York TImes Company, 31 Aug. 2013. Web. 14 Nov. 2013.

outs, citing that only 18% use browser do not track features.[10] Some people will inevitably opt-out (those that care most about their data privacy) while some will correct their data (those that care about the advertisements they see). Most will completely ignore the site, though it has been written about multiple times in publications such as the New York Times.

Howe realizes that his company's self interests are aligned with consumer needs, "We are not going to get anywhere by hiding. You have to make things visible." The new tool, About The Data, is incredibly visible, even educating people on where the data comes from, the aggregation process, and where it goes. Consumers log in with personally identifying information (including the last four digits of their SSN) then can view, edit, or delete the information Acxiom has on them in six sections: characteristic data, home data, household vehicle data, household economic data, household purchase data, and household interest data.[11]

This is a textbook example of revolutionary economist Adam Smith's "invisible hand of the market" theory. Acting in its best interest, Acxiom self-regulates, creating consumer benefits and efficiency in the market. Unfortunately Smith's theory is not as universal as once thought, so imposed regulation is necessary to reach equilibrium in many markets. All Data Brokers cannot be expected to implement open data policies without legislation from the government requiring it, but over time a competitive market without a monopolist will trend towards efficient competition where data brokers and consumers place the same value on their information.[12]

Acxiom is allowing customers to view their data, edit it, and opt-out of profiling if they choose – a strong first step towards transparency. My recommendation is to require such policies from all data aggregators across the country with a reasonable timeline to allow for expenses and resource allocation within the company. As companies adapt, so will consumers and further regulation may be needed for their protection. It would be unrealistic to attempt more stringent regulation in this political environment where lobby firms have the demonstrated ability to stop bills they do not agree with. By starting with a less restrictive but still transparent policy that has been tested already by an American data giant, other companies will not fight the bill as hard as the Kerry-McCain or Right to Know bills.

---

[10] Ibid
[11] "About The Data." *About The Data (Beta)*. Acxiom, n.d. Web. 14 Nov. 2013.
[12] Theory of perfect competition in markets

CONCLUSION

This is a practical, yet effective, solution to the issue that many consumers want to protect their privacy but are ignorant of what data aggregators do with their personally identifying information and accompanying metadata. A bill that proposes transparency and the ability to edit or delete coincides with right to know policies and the Code of Fair Information Practices. It has been proven to work, though at some cost to the data broker, in Europe and by Acxiom. Corporations hold a lot of power in the US, but it is still a democracy for the people. Citizens cannot correctly value their privacy without being educated about what information companies have and what is done with that information, causing them to fall prey to companies that offer marginal perks for personal data. Education and transparency will level this playing field, creating a more just and efficient information market.