Online Consumers and Big Data

Alice E. Marwick
Fordham University, Data & Society
amarwick@gmail.com

Paper prepared for Workshop on Big Data Surveillance, Queens University, May 12-14, 2016

Introduction

The collection of data on consumers by retailers, advertisers, and marketers is nothing new. Market research began in the United States in the 1920s, as industry shifted from manufacturing goods to creating desires. As early as the 1910s, American businesses were surveying small business-owners, analyzing census data for potential insights, and attempting to measure the effectiveness of advertising (Igo, 2007, pp. 110–111). Buying and selling this data, however, did not become a business until the era of affordable computing. In the 1960s and 1970s, marketers began to combine public data, such as telephone directories, with magazine subscription lists and professional associations to create segmented lists of consumers that could be used for direct mail marketing and local political campaigns (Angwin, 2014a, p. 30). A few direct marketing companies merged with credit bureaus, which collect credit information and sell it to banks in order to determine eligibility for financial products, becoming "data brokers" (Schneier, 2015). As information became digital, and computing power became cheaper and more accessible, the ability of data brokers to collect and analyze information sharply increased. The internet, particularly the implementation of cookies in the mid-1990s, amplified the size, scope, and scale of user tracking, and data brokers began to combine personal information gathered "offline" with online information, such as email addresses and web browsing records.

According to a recent report from the US Federal Trade Commission, the lifecycle of "big data" has four parts: collection; compilation and consolidation; data-mining and analytics; and use (Federal Trade Commission, 2016). In this short report, I will focus on the first two phases, specifically with regard to the "data footprints" of individual internet users as they browse the web, use mobile apps, and interact on social media, focusing on *consumer* data. Digital footprints are traces left by individuals as they engage in their everyday digital activities, which are thought by marketers and "big data" advocates to include insights into human behavior and, most importantly, what people might want to buy (Thatcher, 2014). These digital footprints are increasingly combined with data generated during activities offline, such as in-store purchases, loyalty card information, warranties, and even information generated in physical stores, such as length of visit and movement through the store (Anthes, 2014; Clifford & Hardy, 2013); data gathered from social media applications and websites that use "social plugins"; and spatial data generated by mobile phones with GPS devices, or by using mobile apps like Uber (Dalton & Thatcher, 2015). This report discusses *collection:* the activities that generate data

which frames individuals as "consumers," and *compilation and consolidation:* namely, the middlemen, or data brokers, who aggregate, package, and sell that data. I then outline some of the risks that these data collection practices pose, especially to vulnerable populations, and some outstanding questions for the Workshop.

The United States has a mish-mash of regulations which pertain to data collection, but no comprehensive data privacy law. Generally, it has emphasized self-regulation by data industries, while the European Union has enacted more stringent regulations on data collection and storage (Tsesis, 2014). However, since the biggest internet and social media companies are American, its lax approach to regulating data collection and use impacts individuals world-wide. As Sylvia Peacock notes, "Online US business practices set an international precedent on the Internet that seems difficult to reverse. What is more, most governments' desires for people's online information seem well served by the weak or nonexisting policies for the treatment of personal data" (Peacock, 2014, p. 2). While this report focuses primarily on the collection and use of consumer data in the United States, more research is needed on how these practices affect people outside the U.S.

Collection: Sources of Consumer Data

In her book *Dragnet Nation,* journalist Julia Angwin identifies five types of commercial data trackers:

- **Incidental Collectors:** Any business that collects data on its customers, from local dry cleaners to the world's biggest banks.
- **"Freestylers":** software companies which provide "free" services in exchange for customer data.[1]
- **Marketers**
- **Data Brokers:** Companies that buy data from a variety of sources, aggregate and sort it, and sell it to governments, businesses, and individuals.
- **Data Exchanges:** Stock exchange-like trading desks which enable marketers and data-brokers to trade information. (Angwin, 2014a, pp. 32–33)

In this essay, I will examine several types of *incidental collectors* and *freestylers:* social media, smartphones and mobile apps, and online shopping and retail businesses; and *data brokers*, who aggregate information from freestylers and incidental collectors with government and marketing data, among others.

Most online data collection is facilitated by **tracking cookies,** small text files placed on a user's computer or persistent profile by a website.[2] Visiting a website like yahoo.com, for

[1] Professor Joseph Turow argues that this so-called exchange is asymmetrical, that most individuals are unaware of what they are giving up in exchange for "free" services, and that the most aware feel resigned to data collection by companies, even as it makes them uncomfortable. See Turow, Hennessy, & Draper, 2015.

[2] Most modern browsers (Chrome, Firefox, Safari) allow users to "sync" data between devices, meaning that cookies placed on a user's laptop will also track her desktop browsing if she is logged into the browser software.

instance, places cookies from six third-party companies (Conviva, DoubleClick, Innovid, NetRatings SiteCensus, ScoreCard Research, and Sizmek) on the visitor's computer;[3] these companies deliver advertising and analyze site traffic. If the user then visits CNN.com, 22 different third-party cookies are placed on her computer. Since DoubleClick is enabled on both Yahoo and CNN, DoubleClick records her visits to both sites. Third-party cookies thus allow the creation of sophisticated data footprints beyond individual site visits.

Social Media

Social media sites like Twitter, Reddit, Facebook, and Instagram are a rich trove of data, much of which is public. One marketer explained that "If Big Data is the water pouring out of your faucet, then social media is the reservoir that stream comes from" (Hung, 2016). Certainly, the *personal information economy* is fueled by social data (Bennett, Haggerty, Lyon, & Steeves, 2014, p. 11). Some of this data is user-generated, or actively provided by users—status updates, digital pictures, "likes", check-ins, tweets, reviews, "pins", and selfies, to name a few. Notably, even if they do not partner directly with social media sites, many data-brokers crawl or "scrape" websites to harvest user information that is not protected by privacy settings (Federal Trade Commission, 2014). However, still more data is generated passively as individuals move around the web, their actions not only tracked by digital advertising cookies, but by equally ubiquitous social plugins. As a result, social media companies know far more about their users than their users are aware (Trottier, 2012).

Facebook, for instance, has undergone a "vertical expansion" in the types of information it can collect on its users. In addition to its acquisition of Instagram and WhatsApp, which contain rich photo and chat data, respectively, it has added a variety of functionalities to its websites and mobile apps, which allow for more detailed profiling than was previously feasible (Van Alsenoy et al., 2015). Data collected for one purpose can then be used for another, a form of "surveillance creep." For example, if Jane chooses to let Facebook track her location to share that data with friends, this information can also be used to target advertising. Facebook combines user-provided information with information it gets from third parties. News sites, blogs, and content providers are dependent on sites like Facebook and Twitter to spread articles and videos, requiring the integration of "social plugins," the buttons that let you Like, Tweet, or otherwise Share a story on social media. These plugins run scripts that send information to Facebook on what sites their users visit, even if the users do not leave a Facebook comment or a Like. This information is used to target ads more precisely to users (Shaw, 2015). One study found that these plugins even tracked non-users, which Facebook claimed was a "bug" (Gibbs, 2015).[4]

It is not clear, however, whether the data that Facebook collects stays with Facebook. In Facebook's Help Center, they answer, definitively, "No, we don't sell any of your information to anyone and we never will" (Facebook, 2016a). However, Facebook partners with a variety of

[3] Determined by using the Ghostery plugin (ghostery.com)
[4] Facebook has a long history of similar bugs. See Angwin, 2014b.

data-brokers, including Acxiom, DataLogix, BlueKai, Epsilon and Experian, to develop more detailed profiles of users combining on and offline information (Facebook, 2016b; Senemar, 2015). These data-brokers are the largest in the world and already boast masses of data (Acxiom claims to have data on 700 million people; Epsilon a file on every American household; Datalogix "$2 trillion in offline purchase-based data").[5] Combining these data sources with the information that Facebook has on online interactions has allowed the company to develop an ad-targeting system so sophisticated that it "could hypothetically serve soda ads to teenagers who recently purchased a soft drink at a convenience store, or diaper ads to parents who bought baby food at a department store" (Senemar, 2015). Thus, Facebook is not *technically* selling user data, but it is certainly selling advertisers access to user information in unprecedented detail.

Smartphones and Mobile Apps

Mobile devices present a different set of challenges for consumer surveillance than does the web. As the FTC summarized in their 2013 report on Mobile Privacy Disclosures:

> … more than other types of technology, mobile devices are typically personal to an individual, almost always on, and with the user. This can facilitate unprecedented amounts of data collection. The data collected can reveal sensitive information, such as communications with contacts, search queries about health conditions, political interests, and other affiliations, as well as other highly personal information. This data also may be shared with third parties, for example, to send consumers behaviorally targeted advertisements (2013, p. 2).

The FTC goes on to say that mobile devices are part of a complex ecosystem in which information may be shared between operating system providers (Apple's iPhone and Google's Android being the most common), telecommunication providers (such as AT&T, Rogers Wireless, or Virgin Mobile), app and platform developers, advertisers, and analytics firms. Mobile phones are also more intimately connected to individuals than desktops or laptop computers, which can be shared. Data collected through mobile phones is thus deeply personal, hard to protect, and easy to aggregate.

Initially, the shift from desktop-to-mobile browsing presented a problem for online advertisers, in that mobile apps bypassed web-based cookies, thus evading persistent tracking. Wireless providers AT&T and Verizon implemented so-called "zombie cookies," tracking codes which were inserted into all non-encrypted web traffic that any website owner or advertising network could access (Finley, 2015). [AT&T stopped after public protest; Verizon now claims they only track users who go to websites owned by Verizon or AOL (Gillium, 2014)]. An Acxiom whitepaper suggests that unpopular zombie cookies are not even needed, as individuals can be identified through "their authenticated log-in, device identification, or given PII, and then

[5] Datalogix is owned by Oracle Corporation. See Oracle Corporation, 2016.

[by] layering in their past behaviors, affinities, and relationship with your brand" (Acxiom Corporation, 2015, p. 4). In other words, on smartphones which have apps like Google and Facebook installed, individual people can be identified simply by triangulating the multiple data points available, connecting the smartphone user with a pre-existing data profile.

Most importantly, it is the rise of *spatial big data* that presents a sea change in tracking and surveillance for consumer purposes. Spatial data "is predominantly generated through mobile device use, such as smart phones with embedded GPS receivers" (Thatcher, 2014, p. 1768). Since smartphones constantly broadcast their location to provider networks, their location is a "relatively public piece of information" (Landau, 2016, p. 57), and some mobile apps passively track location even if the app is closed, including Google, Facebook, Uber and Foursquare (Halleck, 2014). The addition of location information to digital footprints enables a host of new applications for marketing and advertising. These include physical "conversion tracking," or determining what consumers do after viewing an ad, which may include walking into a physical store to make a purchase (Landau, 2016); and RetailNext's "Shopper Mobile Device Detection," which "makes it possible for [retailers] to leverage the presence of smart phones in your retail environment to collect otherwise unavailable metrics such as visit length, time between visits, and percentage of passersby who come into your stores" (RetailNext, Inc., 2014). Location also affords the creation of more intrusive personal information, such as Uber, who tracked one-night-stands—or what they called "Rides of Glory"—by identifying users who had requested a ride between 10pm and 4am on a weekend night, and were then picked up from their drop-off point just a few hours later (Pagliery, 2014).

Of course, most mobile apps can and do collect data, much of which is sensitive. The "quantified self" movement, which emphasizes self-tracking for personal improvement, has popularized wearable devices and apps that count calories, track workouts, and count steps. This data is valuable to insurance companies, some of which offer discounts to people willing to share their Fitbit data with the company (Mearian, 2015), and US corporate "wellness" programs which require employees to report fitness data to get discounts—or avoid fines (Hamblen, 2015). But it is the aggregation of intimate, biometric, or social material with location information and pre-existing advertising profiles that enables consumer surveillance on an unprecedented scale.

Online Shopping and Retail

Physical retail stores are beginning to use sophisticated technologies to track customers in-person just as they do on-line. Forrester Research warns retailers that "In-store analytics must be leveraged to allow retail stores to operate in a similar way as their online counterparts, leveraging real-time product and shopper behavioral data to drive an improved in-store customer experience (CX) as well as improved operational excellence" (2016). In other words, brick-and-mortar stores need to track individuals as precisely as their websites. This is possible through the use of emerging technologies, including billboards that employ facial recognition technology (Ember, 2016); in-store Wi-Fi and Bluetooth networks that track customer movements throughout stores

regardless of whether customers connect to the network (RetailNext, Inc., 2014); "smart shelves" which can tell what products consumers look at or touch while browsing (Coolidge, 2015); and video cameras which analyze facial cues to determine customers' emotions (RealEyes Data Services Ltd., 2016). The *New York Times* summarizes that retailers are now able "to gather data about in-store shoppers' behavior and moods, using video surveillance and signals from their cellphones and apps to learn information as varied as their sex, how many minutes they spend in the candy aisle and how long they look at merchandise before buying it" (Clifford & Hardy, 2013).

While this data is collected in-person, it is digital, and designed to be aggregated. Data brokers combine data gathered from such retail interactions with pre-existing consumer profiles and online interactions, in a process called onboarding. Anthes writes,

> In onboarding, a data broker will add offline information—data from manual sources or from other systems such as loyalty cards, warranty registrations, and stores' point-of-sale terminals—into the cookies of computers used by individuals to access websites monitored by the broker (2014).

Facebook also engages in onboarding with its Atlas platform, which tracks individuals' unique Facebook IDs across both desktop and mobile browsing, meaning that when someone is logged into Facebook, all the sites in the Atlas network will be able to link your online activity to your Facebook profile (Watson, 2014).

This combination will enable retailers to have extraordinary surveillant powers. Walmart, for instance, has consumer data on more than 145 million Americans, shares online consumer data with 50 third parties, tracks customers throughout stores using wi-fi, and analyzes social media information to link it with specific point-of-sale transactions (The Center for Media Justice, 2013). The ability for data-brokers to link online and offline interactions will require herculean efforts to avoid consumer surveillance.

Compilation and Consolidation: Data Brokers

Consumer data is aggregated by middlemen known as *data brokers.* Data brokers, of which Acxiom is the biggest and best-known, collect, consolidate, and analyze consumer information from social media, retail transactions, direct mail databases, and other sources outlined in the first part of this report, along with information provided by US federal, state, and local governments, including but not limited to: census records; voter registration data; motor vehicle registration and driving records; postal addresses; Most Wanted Lists and terrorist watch lists from the European Union, the US Secret Service, and the Federal Bureau of Investigation; records of bankruptcies; licenses (professional and recreational); tax records; mortgages, liens, deeds, and foreclosures; court records, including births, marriages, divorces, and deaths; contributions to political campaigns; and gun ownership records (Federal Trade Commission,

2014). This information is used to create detailed customer profiles. As noted above, the biggest data brokers claim they have files on every US household. Data brokers use this information for micro-targeting—one data broker sells a list of men suffering from erectile dysfunction, for instance—but also to sort people into categories, or "segments." Experian's Mosaic product sorts Americans into 71 different segments in 19 categories. The FTC criticized brokers for targeting products to "financially vulnerable" segments, the names of which including "X-Tra Needy," "Hard Times," and "Very Spartan" (Federal Trade Commission, 2014).

These profiles are sold to a wide variety of customers. Acxiom claims that its customers include most of the top US credit card issuers, retail banks, telecom/media companies, retailers, automotive manufacturers, brokerage firms, and insurance companies.[6] They also, however, include governments, politicians, and even identity thieves and scam artists. A Vietnamese identity thief bought 200 million records from Experian (Knibbs, 2014). Another data broker bought the financial information from "hundreds of thousands" of payday loan applications, and sold it to "phony Internet merchants" who "raided the accounts for at least $7.1 million" (Reuters, 2015). Such scams are not uncommon given the granularity of data brokers' segmentation. As Gregory Maus writes,

> …Data broker infoUSA was selling lists of 3.3 million 'Elderly Opportunity Seekers' of older people 'looking for ways to make money', 4.7 million 'Suffering Seniors' dealing with cancer or Alzheimer's, and 500,000 'Oldies but Goodies' of gamblers over 55. One list specifically noted that 'These people are gullible. They want to believe that their luck can change.' Naturally, telemarketing fraudsters snapped up these lists like maps to gold mines (2015).

Other brokers have sold lists of rape victims, people with AIDS/HIV, and people with addictive behavior, including alcoholism, drug use, and gambling (Maus, 2015).

Given these abuses, in the last few years, public attention has turned to data brokers, who are no longer as shadowy and invisible as they once were (Anthes, 2014; Beckett, 2014; Tsesis, 2014). The US Federal Trade Commission, the Government Accountability Office, and the Senate Commerce, Science and Transportation Committee released a series of reports and hearings that detailed the practices and operations of data brokers (Cackley, 2013; Federal Trade Commission, 2014; U.S. Senate Committee On Commerce, Science, & Transportation, 2013). However, they remain mostly unregulated in the United States. Separately, there is no way for individuals to view what information data brokers possess on them, and certainly no way to determine whether that information is correct.

[6] http://www.crunchbase.com/company/acxiom#ixzz2iy4tNOK7

Conclusion: Risks and Vulnerabilities

While there are obvious civil rights problems with massive surveillance that exists solely in order to make money for large corporations, there are a number of other risks and vulnerabilities made salient by customer surveillance. It is also important to note that customer data is often purchased by governments and politicians, even if they cannot legally collect it themselves (Marwick, 2014).

Price discrimination, or "digital red-lining," is the most palpable risk of this type of consumer sorting (Podesta, Pritzker, Moniz, Holdren, & Zientz, 2014). Companies already offer discounts to those willing to sign up for "loyalty" programs which generate granular information on buying habits; they may offer products to some consumers and not others, or change prices based on time, date, and location. One experiment found that the cost of a Princeton Review SAT-prep course varied by as much as $1,800 depending on the potential customer's race and zip code (Larson, Mattu, & Angwin, 2015). Data-brokers sort consumers into categories which are based on purchasing power, demographics, and customer habits. Those deemed unworthy—perhaps "Financially Challenged," "Latchkey Leasers" or "Biker/Hell's Angels," may be ignored (Federal Trade Commission, 2014). This could potentially affect an individual's credit score, ability to get a loan, apply for college, or access a variety of other benefits and resources (Podesta et al., 2014).

Jonas Lerman discusses the impacts of exclusion from big data in a *Stanford Law Review* article:

> Those left out of the big data revolution may suffer tangible economic harms. Businesses may ignore or undervalue the preferences and behaviors of consumers who do not shop in ways that big data tools can easily capture, aggregate, and analyze. Stores may not open in their neighborhoods, denying them not just shopping options, but also employment opportunities; certain promotions may not be offered to them; new products may not be designed to meet their needs, or priced to meet their budgets. Of course, poor people and minority groups are in many ways already marginalized in the marketplace. But big data could reinforce and exacerbate existing problems (Lerman, 2013).

While we may consider it advantageous to be "left out" of the "big data revolution," the data harvested by marketers and advertisers will shape "government and the marketplace." The needs of the poor—those without smartphones or debit cards—will be ignored entirely. This could ultimately lead to a decrease in democratic deliberation, or a diminished civic, public culture (Couldry & Turow, 2014). Eli Pariser famously used the term "Filter Bubble" to refer to the ability of social media sites to tailor content based on individual preferences (Pariser, 2011). This could be compounded by the surveillance practices discussed in this report.

Finally, social media data can be extremely revealing. With access only to someone's Facebook Likes, for instance, researchers have been able to accurately predict ethnicity, religion, political orientation, sexual orientation, and drug use, among other demographic information (Kosinski, Stillwell, & Graepel, 2013). One recent study of Twitter was able to determine a user's home location with as little as five geo-tagged public tweets; this information was then used to determine whether an individual was more likely to drink in or outside the home (Hossain et al., 2016). Other researchers have used Twitter, Facebook, and Reddit data to identify people at risk from depression, post-partum depression, post-traumatic stress disorder, anorexia, schizophrenia, and heart disease mortality, among others (Conway & O'Connor, 2016). When combined with other data sources, the potential for social media to bring to light intimate, sensitive, or even confidential information is clear.

It is not only the *size* and *scope* of surveillance that has changed in the era of consumer surveillance. The ubiquity of GPS-enabled cellphones enables detailed location, social, and biometric data to be collected, aggregated with other consumer-related data, and used to create profiles that are unparalleled in their detail and granularity. Such practices deserve a high degree of scrutiny.

Questions

- What groups are especially vulnerable?
- These practices are often framed in terms of *privacy.* What do we gain by framing them as *surveillance*?
- Recently, a group of US privacy and consumer advocacy groups walked out of meetings with retail and marketing industry groups because they were unable to agree on even the most basic standards of consent for facial-recognition software (Singer, 2015). How can we move beyond self-regulation?
- Given that many of the companies pioneering these efforts are from the United States, which has weak data privacy laws, how might EU or Canadian privacy laws be used to impact personal information markets?

References

Acxiom Corporation. (2015). *Recognizing Audiences in the Murky Marketing Ecosystem* (Point of View) (p. 9). Little Rock, AK: Acxiom Corporation. Retrieved from https://facebookmarketingpartners.com/wp-content/uploads/2015/02/AC-0868-14-POV-Murky-Marketing-Ecosystem1.pdf

Angwin, J. (2014a). *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*. Times Books.

Angwin, J. (2014b, June 17). It's Complicated: Facebook's History of Tracking You. Retrieved May 4, 2016, from https://www.propublica.org/article/its-complicated-facebooks-history-of-tracking-you

Anthes, G. (2014). Data brokers are watching you. *Communications of the ACM*, *58*(1), 28–30. http://doi.org/10.1145/2686740

Beckett, L. (2014, June 13). Everything We Know About What Data Brokers Know About You. Retrieved May 4, 2016, from http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you

Bennett, C. J., Haggerty, K. D., Lyon, D., & Steeves, V. (2014). *Transparent Lives: Surveillance in Canada*. Athabasca University Press.

Cackley, A. P. (2013). *INFORMATION RESELLERS: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace* (Report to the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate No. GAO-13-663). Washington D.C.: United States Government Accountability Office. Retrieved from http://www.gao.gov/assets/660/658151.pdf

Clifford, S., & Hardy, Q. (2013, July 14). Attention, Shoppers: Store Is Tracking Your Cell. *The New York Times*. Retrieved from http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html

Conway, M., & O'Connor, D. (2016). Social media, big data, and mental health: current advances and ethical implications. *Current Opinion in Psychology*, *9*, 77–82. http://doi.org/10.1016/j.copsyc.2016.01.004

Coolidge, A. (2015, October 4). Kroger tests "smart shelf" technology. Retrieved May 6, 2016, from http://www.usatoday.com/story/money/nation-now/2015/10/04/kroger-tests-smart-shelf-technology/73320236/

Couldry, N., & Turow, J. (2014). Big Data, Big Questions| Advertising, Big Data and the Clearance of the Public Realm: Marketers' New Approaches to the Content Subsidy. *International Journal of Communication*, *8*(0), 17.

Dalton, C. M., & Thatcher, J. (2015). Inflated granularity: Spatial "Big Data" and geodemographics. *Big Data & Society*, *2*(2), 2053951715601144. http://doi.org/10.1177/2053951715601144

Ember, S. (2016, February 28). See That Billboard? It May See You, Too. *The New York Times*. Retrieved from http://www.nytimes.com/2016/02/29/business/media/see-that-billboard-it-may-see-you-too.html

Facebook. (2016a). Does Facebook sell my information? Retrieved May 5, 2016, from https://www.facebook.com/help/152637448140583

Facebook. (2016b). Marketing Partners. Retrieved May 6, 2016, from https://facebookmarketingpartners.com/marketing-partners/

Federal Trade Commission. (2013). *Mobile privacy disclosures: Building trust through transparency* (FTC Staff Report). Washington D.C.: Federal Trade Commission.

Federal Trade Commission. (2014). *Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission (May 2014)*. Washington, DC: Federal Trade Commission. Retrieved from http://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014

Federal Trade Commission. (2016). *Big Data: A tool for inclusion or exclusion? Understanding the issues* (FTC Report). Washington D. C.: Federal Trade Commission. Retrieved from https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

Finley, K. (2015, October 7). Verizon Curbs "Zombie Cookies," But They'll Still Stalk You. Retrieved May 6, 2016, from http://www.wired.com/2015/10/verizon-curbs-zombie-cookies-theyll-still-stalk/

Forrester Research, Inc. (2016). *Real-Time Data Drives The Future Of Retail: Stores Must Embrace Digital Technologies To Win In The Age Of The Customer* (A Forrester Consulting Thought Leadership Paper Commissioned By RetailNext) (p. 12). Retrieved from http://home.retailnext.net/rs/314-HEV-582/images/Real-Time%20Data%20Drives%20The%20Future%20Of%20Retail_RetailNext-Thought%20Leadership%20Paper.pdf

Gibbs, S. (2015, April 10). Facebook admits it tracks non-users, but denies claims it breaches EU privacy law. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2015/apr/10/facebook-admits-it-tracks-non-users-but-denies-claims-it-breaches-eu-privacy-law

Gillium, J. (2014, November 14). AT&T stops adding Web tracking codes on cellphones | The Big Story. *Associated Press*. Retrieved from http://bigstory.ap.org/article/54128f63044541279214c96a702546a9/att-stops-adding-web-tracking-codes-cellphones

Halleck, T. (2014, August 14). How To Turn Off Smartphone Apps That Track You In The Background. Retrieved May 6, 2016, from http://www.ibtimes.com/how-turn-smartphone-apps-track-you-background-1657868

Hamblen, M. (2015, June 19). Wearables for workplace wellness face federal scrutiny. Retrieved May 6, 2016, from http://www.computerworld.com/article/2937721/wearables/wearables-for-workplace-wellness-face-federal-scrutiny.html

Hossain, N., Hu, T., Feizi, R., White, A. M., Luo, J., & Kautz, H. (2016). Inferring fine-grained details on user activities and home location from social media: Detecting drinking-while-tweeting patterns in communities. *arXiv Preprint arXiv:1603.03181*. Retrieved from http://arxiv.org/abs/1603.03181

Hung, D. (2016, January 22). The Impact of Big Data on Social Media Marketing Strategies. Retrieved May 4, 2016, from http://tech.co/impact-big-data-social-media-marketing-strategies-2016-01

Igo, S. E. (2007). *The averaged American: Surveys, citizens, and the making of a mass public*. Cambridge, MA: Harvard University Press.

Knibbs, K. (2014, March 11). Data brokers accidentally gave an identity thief access to 200 million consumer records. Retrieved May 7, 2016, from http://www.dailydot.com/technology/experian-data-brokers-give-thief-data/

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, *110*(15), 5802–5805. http://doi.org/10.1073/pnas.1218772110

Landau, S. (2016). Choices: Privacy & Surveillance in a Once & Future Internet. *Daedalus*, *145*(1), 54–64. http://doi.org/10.1162/DAED_a_00365

Larson, J., Mattu, S., & Angwin, J. (2015). Unintended Consequences of Geographic Targeting. *Technology Science*. Retrieved from http://techscience.org/a/2015090103/download.pdf

Lerman, J. (2013). Big Data and Its Exclusions. *Stanford Law Review Online*, *66*, 55.

Marwick, A. E. (2014, January 9). How your data are being deeply mined. *New York Review of Books*.

Maus, G. (2015, August 24). How data brokers sell your life, and why it matters. Retrieved from https://thestack.com/security/2015/08/24/how-corporate-data-brokers-sell-your-life-and-why-you-should-be-concerned/

Mearian, L. (2015, April 17). Insurance company now offers discounts -- if you let it track your Fitbit. Retrieved May 6, 2016, from http://www.computerworld.com/article/2911594/insurance-company-now-offers-discounts-if-you-let-it-track-your-fitbit.html

Oracle Corporation. (2016). Audiences: Online Targeting & Segmentation. Retrieved May 6, 2016, from http://www.datalogix.com/audiences/online/

Pagliery, J. (2014, November 25). Uber removes racy blog posts on prostitution, one-night stands. Retrieved May 6, 2016, from http://money.cnn.com/2014/11/25/technology/uber-prostitutes/

Pariser, E. (2011). *The Filter Bubble: What the Internet Is Hiding from You*. Penguin Press HC, The.

Peacock, S. E. (2014). How web tracking changes user agency in the age of Big Data: The used user. *Big Data & Society*, *1*(2), 2053951714564228.

Podesta, J., Pritzker, P., Moniz, E. J., Holdren, J., & Zientz, J. (2014). *Big Data: Seizing Opportunities, Preserving Values*. Washington, D.C.: Executive Office of the President. Retrieved from https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

RealEyes Data Services Ltd. (2016). *Whitepaper : Emotion Management*. Real Eyes. Retrieved from https://docs.realeyesit.com/Realeyes_Whitepaper.pdf

RetailNext, Inc. (2014). *Real Time In-store Analytics withRetailNext* (Data Sheet). San Jose, California. Retrieved from http://retailnext.net/wp-content/uploads/2014/01/RetailNext-Data-Sheet-Real-Time-In-Store-Analytics.pdf

Reuters. (2015, August 12). Data Brokers Sold Payday Loan Applicants' Information to Scammers: FTC. Retrieved May 7, 2016, from http://www.nbcnews.com/business/business-news/data-brokers-sold-payday-loan-applicants-information-scammers-ftc-n408606

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (1 edition). New York, N.Y: W. W. Norton & Company.

Senemar, S. (2015, April 16). Facebook Partners With Shadowy "Data Brokers" To Farm Your Information. Retrieved from https://www.sherbit.io/facebook-partners-with-shadowy-data-brokers-to-farm-your-information/

Shaw, C. M. (2015, April 18). Facebook Tracks Users Without Consent, but Users Can Take Control. Retrieved May 4, 2016, from http://www.thenewamerican.com/tech/computers/item/20688-facebook-tracks-users-without-consent-but-users-can-take-control

Singer, N. (2015, June 16). Consumer Groups Back Out of Federal Talks on Face Recognition [The New York Times]. Retrieved from http://bits.blogs.nytimes.com/2015/06/16/consumer-groups-back-out-of-federal-talks-on-face-recognition/

Thatcher, J. (2014). Big Data, Big Questions| Living on Fumes: Digital Footprints, Data Fumes, and the Limitations of Spatial Big Data. *International Journal of Communication*, *8*(0), 19.

The Center for Media Justice. (2013). *Consumers, Big Data, and Online Tracking in the Retail Industry: A Case Study of Walmart*. The Center for Media Justice, ColorOfChange, Sum of Us.

Trottier, D. (2012). *Social Media as Surveillance: Rethinking Visibility in a Converging World*. Burlington, VT: Ashgate Publishing, Ltd.

Tsesis, A. (2014). Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data, The. *Wake Forest L. Rev.*, *49*, 433.

Turow, J., Hennessy, M., & Draper, N. (2015). *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation*. Philadelphia, PA: The Annenberg School for Communication, University of Pennsylvania. Retrieved from https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

U.S. Senate Committee On Commerce, Science, & Transportation. (2013, December 18). What Information Do Data Brokers Have on Consumers, and How Do They Use It? Retrieved

May 6, 2016, from http://www.commerce.senate.gov/public/index.cfm/2013/12/what-information-do-data-brokers-have-on-consumers-and-how-do-they-use-it

Van Alsenoy, B., Verdoodt, V., Heyman, R., Wauters, E., Ausloos, J., & Acar, G. (2015). *From social media service to advertising network: a critical analysis of Facebook's Revised Policies and Terms*. Leuven, Belgium: KU Leuven Centre for IT & IP Law and iMinds-SMIT. Retrieved from http://lirias.kuleuven.be/handle/123456789/497700

Watson, S. M. (2014, October 7). You, according to your Facebook Atlas ID. Retrieved December 4, 2014, from http://america.aljazeera.com/articles/2014/10/7/facebook-atlas.html