https://doi.org/10.48009/3_iis_2018_92-100
Issues in Information Systems
Volume 19, Issue 3, pp. 92-100, 2018

DATA PRIVACY ISSUES IN THE AGE OF DATA BROKERAGE: AN EXPLORATORY LITERATURE REVIEW

Jamie Pinchot, Robert Morris University, pinchot@rmu.edu
Adnan A. Chawdhry, California University of Pennsylvania, chawdhry_a@calu.edu
Karen Paullet, Robert Morris University, paullet@rmu.edu

ABSTRACT

The creation of digital data is expanding exponentially, and advances in technology have allowed for much of this digital data to be collected and aggregated by data brokers with little effort. Data brokers are selling personal information about individuals for a variety of purposes including marketing, insurance, employee background checks, and government screenings. This exploratory paper reveals several impacts of digital dossiers, including the potential for discrimination and typecasting, as well as misuse of profile data for political, organizational, or personal gain. An interesting finding of the research was the potential negative impacts of digital dossiers that contain inaccurate information, which is not uncommon. Recommendations for future research are discussed.

Keywords: Data Privacy, Information Privacy, Data Brokers, Data Brokerage, Data Surveillance, Digital Dossier

INTRODUCTION

We are living in a time where one does not have complete control of their personal privacy. Some might even argue that people no longer have an expectation of privacy, or at least data privacy. Data privacy is the concept that personally identifiable information (PII) and other data about an individual should only be accessible to authorized parties. Knowing exactly what information is being shared with third parties is often unknown. Information about computer users is being bought and sold by data brokers. Data brokers are companies that are collecting, analyzing and packaging our sensitive and personal information and selling it to companies that are willing to pay (Kroft, 2014). Consumer data collecting is not new; companies have been gathering customer information for decades. People receive unsolicited mail and phone calls as part of targeted advertising and marketing that result from consumer data collection. This has not changed. What has changed is the tremendously increased volume in which data is being mined from personal computers and mobile devices connecting to the Internet, and the improved technical ability to effortlessly collect such a volume of data.

As of April 2017, there were an estimated 3.8 billion Internet users (Kemp, 2017). Each of these Internet users generates a vast amount and variety of digital data each day. According to Forbes, "More data has been created in the past two years than in the entire previous history of the human race" (Marr, 2016, para. 4). It has been estimated that 1.7 megabytes of new information will be created each second of the day for every human on the planet by the year 2020 (Marr, 2016). That is a staggering amount of digital data.

Over the past several decades, a new data brokerage industry has emerged that is based on collecting, processing, and selling personal information (Otto, Anton, & Balmer, 2007; Anthes, 2015). The advance of Internet technology has dramatically impacted this industry, allowing the rapid collection of vast amounts of data that is generated via online website activities and transactions. This data brokerage industry sells information about millions of people to both corporate and government parties. Data brokers now provide comprehensive data profiles called digital dossiers on almost any U.S. adult (Anthes, 2015; Hoofnagle, 2003; Rieke, Yu, Robinson, & Hoboken, 2016).

Data brokers collect personal information on people through public and private sources to include publicly available information from social media, court records, and web surfing (Boutin, 2014). The brokers sell data to clients in reference to a person's ethnicity, income, health status, sexual orientation, and income, to name just a few data points. It is estimated that there are 2,500 to 4,000 data brokers operating in the United States (Boutin, 2014). Companies purchase information from the data brokers to predict patterns of user behavior. For instance, if a person

started to browse the Internet searching sites regarding what to expect during pregnancy, companies can then target that person and send coupons for diapers, baby clothing and more. A notable example of this was in 2012 when the Target retail store was able to identify a teen girl's pregnancy via her browsing and shopping habits before her family was aware of the pregnancy (Hill, 2012; Lubin, 2012). This information being gathered through our personal search habits is being collected and sold to anyone willing to pay.

Harvard Business School professor Shoshana Zuboff calls the mass data collecting by companies "surveillance capitalism" (Zuboff, 2018). Companies such as Google and Facebook offer free services in exchange for a person's data. All of our interests are saved. Google tracks the websites we visit, information pertaining to our Gmail accounts and movements from our mobile devices. Google continuously tracks a person's movements by monitoring our mobile device usage. This constant tracking of people is data surveillance. It is happening without our conscious awareness of the implications of this action. And the data that is being collected from this data surveillance can be startlingly personal. As Schneier notes, "We never lie to our search engines" (Schneier, 2018, para. 6).

This paper will explore the literature surrounding data brokerage and data surveillance, and investigate the known impacts of mass data collection for individuals. This area is just starting to be studied within academia, and thus this exploratory research will address the following questions:

RQ1: How is information collected by data brokers being used?
RQ2: What impacts exist for individuals as a result of the information being collected by data brokers?

Findings from this research will inform future studies to further investigate this critical issue for data privacy. The rest of the paper will be structured as follows. An overview of the types of data brokers and the data that they collect will first be presented. Next, RQ1 will be addressed through a discussion of the uses and potential uses of digital dossiers. RQ2 will be addressed via a discussion of the various impacts of digital dossiers for individuals that were uncovered within the review of the literature. Finally, a conclusion section will identify the contributions of this paper and suggest critical areas for future research.

DATA BROKERS AND THE DATA THEY COLLECT

The Data Brokers

There are a wide variety of data brokers in the U.S., some of which are large-scale and some of which are smaller. There are over 4,000 data brokerage firms worldwide (WebpageFX, 2015), with an estimated 2,500 to 4,000 firms within the U.S. (Boutin, 2014). The data brokerage industry is complex, and there can be some question as to when a company is considered to be a data broker. For example, while some companies gain 100% of their revenue from selling information, other companies may only make part of their revenue from information sales (Rieke, Yu, Robinson, & Hoboken, 2016). In addition, there are layers of data brokers that provide information to each other (Ramirez et al., 2014).

There are three types of data brokerage firms that deal with individuals' information. First are people-searching firms like mylife.com where users can enter personal data for another individual and the site returns results based upon the criteria: either for free or a small charge. On one hand, these sites can be helpful in finding old friends, but of course they may contain information that individuals would prefer to keep private. The second type of firm focuses on marketing and develops digital dossiers on individuals that can be used to target marketing campaigns (Grauer, 2018). Companies purchase these dossiers which include names, email addresses, interests, and offline activity about their prospective customers. The third type of firm can offer risk mitigation products aimed at identifying and protecting against fraud. These are typically the least problematic for consumers unless they are disseminating inaccurate information (Grauer, 2018). For example, financial lenders might use these services to determine if a social security number is associated to a deceased person or whether an address has been associated with fraud. While these can be helpful, they can also create problems for innocent consumers trying to complete a transaction when their address is linked to any fraudulent activity unrelated to them (Grauer, 2018).

Some of the major players in the data brokerage industry include Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf, Recorded Future, Equifax, and ChoicePoint. Acxiom is one of the world's

largest data brokerage firms that has 23,000 servers collecting and analyzing 1.5k data points on over 500 million consumers' data worldwide. This is just an example of the plethora of data that is collected and aggregated. In addition, more than 1,400 store loyalty programs sell your information. The web site "http://intelligence.towerdata.com" contains 80% of U.S. email addresses and 38% of employed Americans' pay stub data is available on Equifax (WebpageFX, 2015).

The Data They Collect

Data brokers collect a wide variety of information on individuals, including name, alias names, social security number, date of birth, and telephone numbers. This information is often referred to as personally identifiable information (PII). But, digital dossiers of individuals do not stop with PII. Dossiers collected by data brokers also contain a wealth of information about an individual's demographic data, employment history, court and public records history, social media data, financial data, travel data, purchase behavior and real estate and vehicle ownership (Mirani & Nisen, 2014). This includes current and past employers, vehicles, driver's license information, professional licenses, concealed weapons permits, liens, legal judgments, arrest and court records, lawsuits, marriages, divorces, and worker's compensation claims (Hoofnagle, 2003). This larger set of data contained in a digital dossier is often referred to as sensitive personal information (SPI) and can be used on its own or in combination with PII to identify, locate, or contact an individual.

Data from individuals is collected from public records and other public sources, but also from non-public government and commercial sources. This could include voting registration, bankruptcies, consumer purchase data and other web browsing activities (Ramirez et al., 2014). In addition, data can be gleaned from email accounts, social media posts, and personal websites (Anthes, 2015). Otto, Anton, and Balmer (2007) report on the various sources from which ChoicePoint acquires its data, including: Federal government, State government, local government, National Credit Bureaus, phone companies, law enforcement, the court system, insurance companies, and unknown sources. From the federal government, a variety of data points were gathered including: "shareholder status, trademarks owned, pilot licenses, aircraft registrations, Marine radio licenses, controlled substances licenses, Firearms and explosives licenses, and military records" (Otto, Anton, & Balmer, 2007, p. 3). State governments provided: "Business loans, businesses owned, vehicle registrations, boat registrations, driver's license number, driving record, professional licenses, fishing licenses, marriages and divorces, birth and death certificates" (Otto, Anton, & Balmer, 2007, p. 3). Local government provided: property ownership, deed transfers, and property values. National credit bureaus supplied a variety of PII including name, known aliases, social security number, date of birth, current addresses, past addresses, and credit history. Telephone numbers were accessed by phone companies. Law enforcement provided: "police reports, criminal records, FBI sex-offender and wanted-criminal lists, suspected terrorist lists, and criminal fingerprints" (Otto, Anton, & Balmer, 2007, p. 3). Insurance companies supplied worker's compensation claims as well as home and automobile insurance claims. Unknown sources provided the names and addresses of relatives and neighbors, as well as education and employment history (Otto, Anton, & Balmer, 2007). These are data points collected from various public sources by ChoicePoint, but they serve as an example of the types and amount of data available on individuals that are being collected by other data brokers as well.

Data Collection Without Consent

Equifax is a consumer credit reporting agency which collects and aggregates information on over 800 million individual consumers and over 88 million businesses worldwide (Equifax, 2018). Equifax is one of the three major credit reporting agencies from which people obtain their credit scores. In September 2017, Equifax exposed 143 million Americans sensitive personal information in a data breach. Hackers accessed people's names, social security numbers, birth dates, addresses, and in some instances driver's license numbers. Credit card numbers of over 209,000 people were also exposed (FTC, 2017). This may sound like another familiar breach but one thing is different. Equifax, the company that should have been protecting consumer data, is in fact a data broker buying and selling user information without our knowledge.

In March of 2018, the Facebook Cambridge Analytica scandal was brought to public attention. The personally identifiable information (PII) collected from 87 million Facebook users was used by Cambridge Analytica, a data brokerage firm, to allegedly influence voter opinions. The way that Cambridge Analytica collected the data was called "inappropriate." This is the largest leak of data in Facebook's history (Confessore, 2018). Cambridge Analytica paid Facebook users a small amount of money to download an app called "This Is Your Digital Life"

where they would be prompted to take surveys. Data was collected not just from the users of this app on Facebook, but also from the users' friends (who did not sign up for the app). The app, in its terms of service, disclosed that it would collect data on the users and their friends (Bloomberg, 2018). Facebook is under fire for allowing the app developer to collect information on a user's friends. After Facebook became aware of the company's collecting practices they asked Cambridge Analytica to destroy the information. The data was not destroyed. In the United Kingdom, where Cambridge Analytica is headquartered, there are protection laws that ban the sale of personal data without consent. Those same laws do not exist in the United States.

Though much of the data collected by data brokers is publicly available, it is still collected without the consumers' knowledge or consent (Anthes, 2015; Ramirez et al., 2014). In addition, data collected is aggregated from a variety of sources in order to provide a more detailed picture about a particular person (Ramirez et al., 2014). This can be misleading even for privacy-savvy consumers who believe that small amounts of data disclosed to one source are harmless, not realizing that this data, when aggregated, can be much more privacy-invasive.

Other types of data that are collected are user-generated. Some of the data generated is done intentionally and knowingly, such as posting to a social media site, adding a comment to an online article, or making an online transaction such as a purchase or money transfer. But the majority of this data is being generated behind the scenes as metadata that is captured when users interact with mobile apps and websites, and from sensors embedded in smartphones, smartwatches, fitness trackers, home assistant devices such as Amazon Echo or Google Home, and other electronic devices. This metadata that is being recorded is not readily apparent to the user. Llorca-Abad and Cano-Oron (2016) argue that many Internet users do not realize the loss of control over their data, due to both a lack of digital literacy and the quiet approach with which the data is collected behind the scenes. Ramirez et al. (2014) note, "Data brokers do not obtain this data directly from consumers, and consumers are thus largely unaware that data brokers are collecting and using this information" (p. iv).

USES OF DIGITAL DOSSIERS

Information collected about individuals by data brokers is being used in a variety of ways including marketing and advertising services, insurance background checks, employee background checks, government screenings, and more.

Data brokerage firms collect data from public sites and online activity for marketing purposes (WebpageFX, 2015). This data is used by companies to target customers with their advertisements. For example, if you search on a search engine several times for trips to Europe, you may then find targeted advertising focused around trips to Europe appearing in your own news feeds, search engines, and social media sites. While some users are concerned about this invasion of privacy, many users appear unconcerned and willing to trade the convenience of online services for information about themselves that will be used for marketing (Morgan, 2014; Phelps, Nowak, & Ferrell, 2000).

But, marketing is not the only use for which data brokers are selling user data. As an example, ChoicePoint sells data to a variety of customer sectors including insurance providers, corporate entities seeking employee background checks, government entities seeking Homeland Security screenings, marketing services, and other (Otto, Anton, & Balmer, 2007).

In 2012, the data broker industry generated 150 billion dollars in revenue which was twice the size of the entire intelligence budget for the U.S. Government. One data broker sold a list of one thousand individuals with health conditions like anorexia, substance abuse, and depression for just $79. Today, data brokering is over a $200 billion industry where the average email address is worth $89 to a brand or marketing effort over time (WebpageFX, 2015).

Consumers are not completely powerless around data brokers in regard to collecting their personal information. Forty-three percent of data brokers allow consumers to opt out for free (monetarily speaking), although it can be time-consuming and not worth the effort to keep your data from being sold (WebpageFX, 2015). However, if you are okay with the idea of data brokerage firms collecting your data, there are companies like Datacoup which collect information on you as a consumer and ensure proper data is being disseminated to external organizations.

IMPACTS OF DIGITAL DOSSIERS

A variety of potential negative impacts of digital dossiers have been identified for individuals. Some of these impacts include the misuse of profile data: to discriminate against a person or typecast a person based on their characteristics or online behaviors, to use collective data for political, organizational, or personal gain, or to foster an oppressive government or corporate environment that thrives on the ability to collect too much information about individuals. Another interesting impact of digital dossiers is the concept of perpetuating inaccuracies. If there is inaccurate information in a person's digital dossier, it could severely impact that person's business, education, retail, health, and government-related transactions.

Discrimination and Typecasting

Digital dossiers could be hugely impactful to a person in a negative way if the information is misused in order to discriminate against a person. While the Federal Trade Commission's study of data brokers in 2014 (Ramirez et al., 2014) found that users are most often put into relatively innocuous "categories" such as "pet owner" or "football enthusiast," other categories gleaned from the digital data can be more problematic, such as "'single mom struggling in an urban setting' or 'people who did not speak English and felt more comfortable speaking in Spanish' or 'gamblers'" (Naylor, 2016, para. 9). Digital dossiers could have major impacts on job seekers, educational program applicants, politicians, and others.

Inaccurate Digital Dossiers

Data brokers can easily typecast a person in any number of ways, even if the data on which their assumptions are based is incorrect (Llorca-Abad & Cano-Oron, 2016). For example, job seekers may be turned away based on a bad credit record, or physical characteristics and health issues that could be seen to affect job performance (Llorca-Abad & Cano-Oron, 2016). Health or life insurance policies may be impacted by data collected in a person's digital dossier purchased from a data broker. The information in a digital dossier in these cases might come from metadata collected from online web sites, mobile apps, and fitness tracking devices. But what if the information in a digital dossier is incorrect? Perhaps a true mistake was made while saving or transmitting data from a web site or mobile app. Or perhaps the data saved was a mistake in a less obvious way. For example, a spouse, relative, or friend might use a person's smartphone, smartwatch, or fitness tracker and data that is recorded during that time will be inaccurately reflected on the owner of the device, rather than the user of the device. This is only an example, but illustrates a very important issue. A plethora of health-related information is now being created outside of HIPAA protection, primarily by patients using various fitness and health tracking devices, mobile apps, and websites (Glenn & Monteith, 2014).

Data brokers are using what is called "consumer scores." A consumer score is a computer-generated number that uses predictive analytics to determine a person's likelihood to get sick or even to pay their bills on time. Predictive analytics uses data mining, statistics and machine learning to make predictions about the future. Consumer scores are similar to FICO scores, but are not regulated in determining the contributing factors of the score (Boutin, 2016). The World Privacy Forum has reports on consumer scoring (World Privacy Forum, 2018). National health plans are using a person's online shopping behavior to determine an individual's rate for health insurance. For instance, a woman who shops frequently online was predicted to be a high health risk whereas, a couple who purchased hiking boots was considered a lower health risk, therefore lowering the price of their health insurance. In this scenario, it is possible that the couple purchased the boots for their children or even a friend. Data collected is often incorrect yet is being used to determine consumer scores. Axciom is considered to be one of the best data brokerage companies yet they carry only a 50% accuracy rate (Boutin, 2016). Clients of data brokers are using this inaccurate data to predict patterns.

Incorrect data in a digital dossier is not uncommon. A reporter from The Atlantic noted that in a review of a data broker's report on herself, nearly 50 percent of the data in the report was incorrect (Miller, 2017). Lucker, Hogan, and Bischoff (2017) conducted a survey to gauge the types of big data inaccuracies and consumers' willingness to update incorrect data about them. Two thirds of the respondents stated their information was less than 50% accurate. One third of the respondents stated that their data was less than 25% accurate. Forty-two percent of the participants stated their online purchase activity had inconsistencies (Lucker, Hogan, Bischoff, 2017). In this study participants were asked to identify categories where they found their data to be inaccurate. Of the participants who found their data accuracy to be less than 50% accurate, also provided responses on which categories had

inaccuracies. The results of this analysis for each category was 84% for economic data, 75% for vehicle data, 59% demographic data, 54% Interest related data, 49% purchase history data, and 41% home related data.

The participants were asked if given the opportunity, would they correct the inaccurate data about them. Only about half of the people who found inaccurate data responded they would change the data about them. The most common reason given by about 31% of the respondents who chose to edit their information was that the information was inaccurate and they wanted to correct that. The second most common reason given by 17% of the respondents who opted to fix their inaccurate information was to correct only those parts they found relevant or beneficial to them. Only 11% of the respondents wanted to edit their data due to concerns about privacy and nervousness about having their information publicly available. Some respondents stated their desire to simply reduce or avoid targeted marketing and political mailings would be sufficient reason to edit their data (Lucker, Hogan, and Bischoff, 2017).

While individuals should be concerned with their data being incorrect, organizations who acquire data from these brokerage firms should share this concern given their efforts could be misguided and lead to missed opportunities. For example, organizations can lose out on customer loyalty and revenue by incorrectly targeting customers with marketing initiatives that do not relate to them (Lucker, Hogan, and Bischoff, 2017). This may include pushing customers along too fast, assessing a customer's profile or risk incorrectly, and even predicting an outcome incorrectly. If an organization launches a new product aimed at individuals with lower credit scores and accidentally targets higher credit individuals, they have likely wasted resources and money on a campaign that is likely to fail.

Using inaccurate data can be a major problem for companies that are using the data to build relationships with their consumers, especially if they are relying heavily on the data or in some cases using it blindly. In an article published by Deloitte Insights, Nate Silver quoted the following in regards to our love affair with big data: "We're not that much smarter than we used to be, even though we have much more information - and that means the real skill now is learning how to pick out the useful information from all this noise" (Lucker, Hogan, and Bischoff, 2017).

Lack of Regulation

Data brokers operate in an environment that is largely unregulated (Otto, Anton, & Balmer, 2007). Hoofnagel (2003) argues that there are significant risks to privacy that are raised by the massive collection of data on individuals. Among these risks are the uses of this collective data for political, organizational, or personal gain. Hoofnagel (2003) also states a concern about the possible uses of collective data by government, noting, "There is also a general risk that the collection of information on individuals will upset the balance between government and individuals, resulting in a shift of power that is oppressive" (p. 596-597). This risk can also be seen for the employer-employee relationship. In a report written by the Federal Trade Commission (FTC), they recommends that Congress should enact regulation requiring data brokers to be more transparent and give consumers greater control over their personal information(FTC, 2014). The FTC suggests the following:

- There should be a centralized portal where data brokers can identify themselves and their data collection practices
- Require data brokers to give consumers access to their data
- Require Opt-In, Opt-Out options
- Data brokers should tell consumers what has been derived from their data collection
- Data brokers should be required to disclose the names and categories of their data sources, allowing consumers to determine if the sources are accurate
- Consumer entities such as retailers should be required to notify consumers of what they are sharing and with whom
- Further protection of sensitive data such as health information should require express consent of the individual (FTC, 2014)

CONCLUSIONS

It is clear that there are a variety of issues relating to privacy that need to be addressed in the data brokerage industry. Data brokers should be transparent in their dealings with consumers (Ramirez et al., 2014) and provide simple solutions for individuals review their aggregated profiles and to opt out of data collection. While the call for transparency is clear, the procedure for achieving it may be less so. Due to the complex nature of the data brokerage industry, and the fact that many data brokers are not solely data brokers, it can be difficult for individuals to know which companies are collecting their data behind the scenes. In addition, the lack of digital literacy and the continuing plethora of electronic devices connecting to the Internet exacerbate this problem. Many "smart" devices today that are part of the connected Internet of Things (IoT) can collect data via sensors and automation that is largely undetected by consumers. Even technology-savvy individuals may not realize all of the ways their devices and online actions are generating data about them. The quiet data collection behind the scenes seems unethical even though it may technically be legal. Transparency in data brokerage processes in the future will be key, and awareness training for individuals and companies on these issues will be paramount.

Future studies will be needed in this area to further understand consumer awareness of the ramifications of online data collection and data brokerage. In addition, research needs to further investigate the inaccuracies in digital dossiers and how these inaccuracies may impact individuals in the future. Additionally, future studies can evaluate participants' willingness to edit inaccurate data about themselves, the level of interest in sharing specific information, and a historical evaluation of how data collection and brokerage firms have impacted their lives. Lastly, future research can also understand and evaluate the impact to the third-party organizations that consume this data. It would be important to understand how they consume it, if they vet the data, and the impact (positive and negative) this data has on their organizations.

REFERENCES

Anthes, G. (2015). Data brokers are watching you. *Communications of the ACM, 58*(1), 28-30.

Bloomberg. (2018). Facebook cambridge analytica scandal: 10 questions answered. Retrieved on May 8, 2018 from http://fortune.com/2018/04/10/facebook-cambridge-analytica-what-happened/

Boutin, P (2016). The secretive world of selling data about you. Retrieved on May 1, 2018 from http://www.newsweek.com/secretive-world-selling-data-about-you-464789

Confessore, N. (2016). Cambridge analytica and facebook: The scandal and the fallout so far. Retrieved on May 6, 2018 from https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Croft, S. (2014). The data brokers: Selling your personal information. Retrieved on May 6, 2018 from https://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/

Federal Trade Commission (2014). FTC Recommends congress require the data broker industry to be more transparent and give consumers greater control over their personal information. Retrieved on May 11, 2018 from https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more?utm_source=govdelivery

Federal Trade Commission (2017). The equifax data breach: what to do. Retrieved on April 30, 2018 from https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

Glenn, T., & Monteith, S. (2014). Privacy in the digital world: Medical and health data outside of HIPAA protections. *Psychiatry in the Digital Age, 16*(494). 1-11.

Grauer, Y (2018). What are Data Brokers, and Why are They Scooping Up Information About You?. Retrieved on May 2, 2018 from https://motherboard.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection

Hill, K. (2012). How Target figured out a teen girl was pregnant before her father did. *Forbes.* Retrieved from https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#3cd9d8746668

Hoofnagle, C. (2003). Big brother's little helpers: How ChoicePoint and other commercial data brokers collect and package your data for law enforcement. *N.C.J. Intl' L. & Com. Reg., 29*, 595-637.

Kemp, S. (2017). The global state of the internet in April 2017. Retrieved from https://thenextweb.com/contributors/2017/04/11/current-global-state-internet/#.tnw_iUhkTTm1

Llorca-Abad, G., & Cano-Oron, L. (2016). How social networks and data brokers trade with private data. *Revista de Estudios para el Desarrollo Social de la Comunicacion, 14*. 84-103. Retrieved from http://revista-redes.hospedagemdesites.ws/index.php/revista-redes/article/view/454

Lubin, G. (2012). The incredible story of how Target exposed a teen girl's pregnancy. *Business Insider.* Retrieved from http://www.businessinsider.com/the-incredible-story-of-how-target-exposed-a-teen-girls-pregnancy-2012-2

Lucker, J., Hogan, S., & Bischoff, T. (2017). Predictably Inaccurate: The Prevalence and Perils of Bad Big Data. Retrieved on May 3, 2018 from https://www2.deloitte.com/insights/us/en/deloitte-review/issue-21/analytics-bad-data-quality.html

Marr, B. (2016). 20 mind-boggling facts every business leader must reflect on now. Forbes. Retrieved from https://www.forbes.com/sites/bernardmarr/2016/11/01/20-mind-boggling-facts-every-business-leader-must-reflect-on-now/#20f5c48820dc

Miller, C. (2017). I bought a report on everything that's known about me online. *The Atlantic.* Retrieved from https://www.theatlantic.com/technology/archive/2017/06/online-data-brokers/529281/

Mirani, L., & Nisen, M. (2014). The nine companies that know more about you than Google or Facebook. Retrieved on May 11, 2018 from https://qz.com/213900/the-nine-companies-that-know-more-about-you-than-google-or-facebook/

Morgan, J. (2014). Privacy is completely and utterly dead, and we killed it. *Forbes.* Retrieved from https://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/#615c9df031a7

Naylor, B. (2016). Firms are buying, sharing, your online info. What can you do about it? *NPR.* Retrieved from https://www.npr.org/sections/alltechconsidered/2016/07/11/485571291/firms-are-buying-sharing-your-online-info-what-can-you-do-about-it

Otto, P., Anton, A., & Baumer, D. (2007). The ChoicePoint dilemma: How data brokers should handle the privacy of personal information. *Security & Privacy, IEEE, 5*, 15-23.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19(*1). 27-41.

Ramirez, E., Brill, J., Ohlhausen, M., Wright, J., & McSweeny, T. (2014). Data brokers: A call for transparency and accountability. *Federal Trade Commission*, i-110.

Rieke, A., Yu, H., Robinson, D., & Hoboken, J. (2016). Data brokers in an open society. *Open Society Foundations*, 1-64.

Schneier, B. (2018). It's not just Facebook. Thousands of companies are spying on you. Retrieved from https://www.cnn.com/2018/03/26/opinions/data-company-spying-opinion-schneier/index.html

WebpageFX (2015). What are Data Brokers – And What is Your Data Worth?. Retrieved from https://www.webpagefx.com/blog/general/what-are-data-brokers-and-what-is-your-data-worth-infographic/

World Privacy Forum, (2018). World privacy forum retrieved on May 8, 2018 from https://www.worldprivacyforum.org/about-us/

Zuboff, S. (2018). The age of surveillance capitalism: The fight for a human future at the new frontier of power.