# Issues in Data Privacy: A Religious Perspective on a Modern Problem

Presented to the S. Daniel Abraham Honors Program in Partial Fulfillment of the Requirements for Completion of the Program

Stern College for Women
Yeshiva University
May 6, 2020

Rachel Leiser

Mentor: Professor Alan Broder, Computer Science

**Table of Contents**

## I. Introduction

All businesses use data, and all individuals contribute to this data- whether they know it or not. Over the last few decades, as the amount of data collected on the internet has increased drastically, the amount of data used by businesses has increased as well. With more data, businesses are able to reach wider audiences than ever before and create more meaningful impacts with their work. Whether deciding where to open a next franchise or deciding when the best time is to release a new product, businesses are able to use data to increase customer engagement and satisfaction in order to flourish in ways that were never possible in the past.

Although there are many positive aspects to collecting and using online data, there are many negative consequences concerning the availability of online data – when more data is accessible, there are more opportunities for data exploitation. As online data accumulates, and individuals lose control of the personal information or data that circulates about themselves, the threat to individual privacy increases. Although laws exist to protect online privacy, the ever-changing online data landscape is moving in a direction that is difficult to predict. The laws, therefore, are not all-encompassing and issues are constantly arising that have never existed before. As the collection, and therefore availability, of data continues to grow at extreme rates, it is crucial to recognize and learn more about the potential usages of online data in order that, moving forward, society is able to better protect individual privacy, and individuals are able to better protect themselves. Because the concept of privacy has expanded in the digital age, it is also important to explore Jewish law as it relates to privacy as online data continues to grow, in order to ensure that it incorporates all relevant and contemporary issues. After analyzing the various issues accompanying the availability of online data, we can look to Jewish law for a framework that will allow us to avoid some of these issues, thereby reducing the danger that the issues of online data pose to all of society.

## II. How Are Companies Using Data?

Data is an extremely powerful tool that allows companies to make efficient, business-savvy decisions. Using data wisely allows companies to reduce costs and increase profits in ways that were not possible before data collection became a widespread practice. One example of a company that relies on data in an effort to drive business decisions is Starbucks. In 2019, the Starbucks mobile app had 25.2 million users.[1] Each one of these users contributes to the massive amounts of data that the company uses in order to make decisions about what products they will sell, where they will sell those products, and how those products will be sold. When users sign up for the Starbucks mobile app, they authorize Starbucks to gather various information about their activity within the app. Because the app collects information about users' preferred orders, it is able to use this data in its sophisticated cloud-based artificial intelligence engine, called the Digital Flywheel Program, to provide personalized recommendations of new products to individual users who "didn't even know, yet, they wanted to try something new."[2] The complex artificial intelligence system is even programmed to consider factors such as weather conditions, day of the week, and time of day when making these personalized recommendations. Starbucks uses data as simple as an individual's daily coffee order in driving their marketing and business decisions in an effort to largely improve the customer experience.

Another company that is attempting to use data to improve the customer experience is Netflix. On December 10, 2017, Netflix tweeted: "To the 53 people who've watched A Christmas Prince every day for the past 18 days: Who hurt you?" While perhaps this was Netflix's way of lightheartedly connecting with their Twitter audience, this tweet actually reveals information about the kind of data that the world's leading streaming entertainment

service collects and uses as part of their research, and eventually marketing, efforts. There is an entire website at Netflix devoted specifically to their research. One of these research areas is called 'Analytics', whose focus is on 'driving insights from data'. According to research.netflix.com,

> Netflix has been a data-driven company since its inception. Our analytic work arms decision-makers around the company with useful metrics, insights, predictions, and analytic tools so that everyone can be stellar in their function. Partnering closely with business teams in product, content, studio, marketing, and business operations, we perform context-rich analysis to provide insight into every aspect of our business, our partners, and of course our members' experience with Netflix.

Like Starbucks, Netflix utilizes user data in order to enhance the customer experience by making the Netflix experience a more personalized one. When someone uses Netflix to stream a movie or a TV show, the next time they log onto the website, they will notice a section on the homepage titled 'Top picks for [user name]', that will contain titles of TV shows or movies that Netflix recommends to the user based on previous programs that they have watched.

Another creative way that Netflix uses data to provide personalized recommendations is through interactive TV. In December 2018, Netflix released a program titled 'Bandersnatch'. In this hour-and-a-half episode of the 'Black Mirror' series, the viewer participates in creating the storyline; as the viewer watches, he or she is asked to make decisions about what will happen next. For example, at one point in the episode, the viewer is asked whether a murder should be committed, and if the viewer answers 'yes', the viewer must decide if the body should be buried or chopped up. It seems that the idea for an interactive show such as this one is simply to create an improved user experience when watching this specific show- the assumption is that if the viewer is the one to decide what happens next, the viewer will care more about the show. In reality, filmmakers can actually take data that is collected from an individual's choices that were made when watching an interactive program such as Bandersnatch in order to guide their efforts in making personalized recommendations. When

the viewer is forced to choose what should be done with the body following the murder, if the viewer chooses to chop up the corpse, Netflix might label the viewer as someone who might enjoy a gory horror movie. When many such choices are made throughout a program, an entire psychological profile can be built up about the user and ultimately be used to make recommendations about the types of programs they might enjoy watching.[3] Ultimately, if the viewer is constantly being given suggestions of TV shows or movies that they might enjoy, and these suggestions turn out to be accurate, they will continue to use the streaming service.

## III. Laws Surrounding Online Data

While the collection and usage of data that is done by companies such as Netflix and Starbucks might seem innocent, and maybe even an enhancement of the consumer experience, there are various issues that are presented with data collection, the biggest one being that it is a violation of the peoples' right to privacy. Although the United States Constitution does not explicitly mention a right to privacy, the Supreme Court has found that there are various amendments that imply privacy rights; for example, the Fourth Amendment protects against unreasonable searches, and the Fifth Amendment protects against self-incrimination.[4] In 1890, Louis Brandeis, a lawyer who would later become an associate justice on the Supreme Court, along with his partner, Samuel Warren, published "The Right to Privacy", which was the first major article to advocate for a legal right to privacy. In the article, the authors describe the right to privacy as "the right to be let alone". According to the Encyclopedia Britannica, the 'right to privacy' which is expressed in the U.S. Constitution, as well as by Brandeis and Warren, "asserts a right of persons to recover damages or obtain injunctive relief for unjustifiable invasions of privacy prompted by motives of gain, curiosity, or malice."[5] As

society and technology have progressed since the publication of this article in 1890, the understanding of and the laws surrounding the right to individual privacy have expanded.

Many companies take user data without informing the user what data they are taking and how they plan on using it. Because of this, there are laws across the United States, as well as in other countries, to protect individuals against data privacy concerns that arise with the increasing collection of online data. Perhaps the most comprehensive privacy law in the United States is the California Consumer Privacy Act (CCPA), originally enacted in 2018. Under this law, users have the right to know what data is being collected about them and why it is being collected. They also have the ability to opt out of their data being sold to third parties, and the right to access any of their stored data or to request that a business delete personal information about themselves that has been collected. Finally, under this law, businesses cannot discriminate against any consumers who choose to exercise any of the rights outlined in the privacy act.[6]

Similar to the CCPA, the European Union also has a version of a data privacy and security law called the General Data Protection Regulation (GDPR). This regulation was put into effect in May 2018, and according to its website, it is the toughest privacy and security law in the world. According to the GDPR, anyone who processes data must adhere to seven protection principles: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability. The fines for violating the GDPR can be as high as 20 million Euro, or 4% of global revenue (whichever is higher). The GDPR outlines when you are allowed to process data, such as when the subject gives specific, unambiguous consent or when processing data is necessary to save someone's life. The GDPR also describes the data subjects' privacy rights, which include the right to be informed, the right of access, and the right to erasure. Although this law was passed

by the EU, its obligations are imposed upon any business in any location that targets or collects data from people in the EU.[7]

In contrast to the GDPR in the European Union, in Canada, a privacy law called the Personal Information Protection and Electronic Documents Act (PIPEDA) was enacted which, although containing many similarities to the GDPR, has fewer stringencies. Similar to the GDPR, under PIPEDA, organizations must obtain consent when they collect, use or disclose an individual's personal information, and individuals have the right to access their personal information. One difference between GDPR and PIPEDA, however, is that extraterritoriality is not mentioned explicitly in PIPEDA; while in the EU, even companies that are not located in the EU must still adhere to the specifications of GDPR if they are targeting members of the EU, this is not specified in PIPEDA; according to PIPEDA, if a business is located outside of Canada, they may not need to comply with PIPEDA even when targeting Canadian subjects. Another difference between Canada's PIPEDA and the EU's more comprehensive GDPR is that under the GDPR, individuals can request for their personal information to be deleted, while under PIPEDA, individuals have the right to withdraw consent for data collection, but they may not be able to have the company delete the data before they have completed using it for the purpose for which it was collected.[8]

With the increasing availability and popularity of online data collection, the laws around the world are constantly being amended to accommodate the needs of various businesses, but more importantly, the needs of individuals to maintain privacy in a world where personal data is being used at alarmingly high rates.

## IV. Issues that Arise from Online Data

### *a. Dangers of Publicly Available Data*

In addition to the various data privacy laws that exist within the US to protect the rights of individuals who provide data to private businesses, there is also a law that is intended to address an individual's 'right to know' when it comes to their data that is collected by government organizations. The New York State's Freedom of Information Law (FOIL) provides a process that allows for members of the public to access records of governmental agencies.[9] Although this law exists in order to protect individuals and provide them with the information that belongs to them, in reality, many issues arise with the public availability of such data that can ultimately be detrimental to a person's privacy.

One example of a dataset that was released due to FOIL in 2014 is the set of New York City taxi data. This dataset contains details of all New York City taxi rides that took place during the year 2013 and onwards, including pickup and drop-off times, locations, and fare/tip amounts. Due to the FOIL law, Chris Wong, who describes himself on his website as a 'data junkie', was able to obtain 20 gigabytes of data which included information on 173 million taxi trips. While city officials thought they had anonymized the data enough by hiding certain details associated with each taxi ride, analysts were able to bypass precautions taken by the city, revealing far more information about individuals than the city had hoped when they released their data.

Anthony Tockar, a graduate student at Northwestern at the time, showed just how invasive to personal lives that this dataset actually was. Tockar noted that many photographs are posted online of celebrities getting into and out of taxis in New York City. Using both taxi medallion numbers and license plate numbers, as well as timestamps, Tockar was able to pinpoint exactly where certain celebrities went, how much the ride cost, and how much they tipped their driver. Examples of such celebrities whom he was able to gather information about

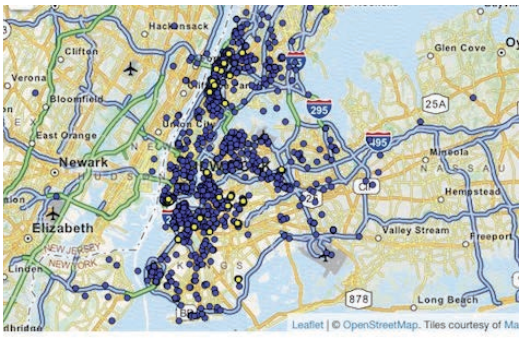
include Bradley Cooper and Jessica Alba. In a blogpost written by Tockar for Neustar, the firm for which he was interning at the time, he summarized his findings as follows:

> In Brad Cooper's case, we now know that his cab took him to Greenwich Village, possibly to have dinner at Melibea, and that he paid $10.50, with no recorded tip. Ironically, he got in the cab to escape the photographers! We also know that Jessica Alba got into her taxi outside her hotel, the Trump SoHo, and somewhat surprisingly also did not add a tip to her $9 fare. Now while this information is relatively benign, particularly a year down the line, I have revealed information that was not previously in the public domain. Considering the speculative drivel that usually accompanies these photos (trust me, I know!), a celebrity journalist would be thrilled to learn this additional information.

Tockar acknowledges that celebrity cab data might seem harmless, or maybe just irrelevant to the average person, but he also illustrates how availability of such taxi data might be harmful to an individual. Tockar looked at Larry Flynt's Hustler Club which is located in an isolated location in Hell's Kitchen in New York City and ran a query that pulled out all taxi pickups that occurred at this location between the hours of midnight and 6 am. A SQL query to do this is simple; it takes as little as six short lines of code in order to pull out such taxi trips. Such a query might be as follows:

```
WHERE pickup_latitude > 40.767249 AND pickup_latitude < 40.7706
    AND pickup_longitude > -73.996782 AND pickup_longitude < -73.9
    AND HOUR(pickup_datetime) < 6
    AND trip_distance > 5;
```

From the data that is pulled using this query, Tockar was able to create a map of drop-off coordinates in order to pinpoint individuals who frequent Larry Flynt's Hustler Club.



When mapping the drop-off points, it is likely that a person who lives in a location which contains very closely clustered drop-off points, denoted in this map by the yellow points, is a frequent customer. Tockar details the harm of such data being available as follows:

> Examining one of the clusters in the map above [referencing the map that Tockar created showing the drop-off points from the Hustler Club] revealed that only one of the 5 likely drop-off addresses was inhabited; a search for that address revealed its resident's name. In addition, by examining other drop-offs at this address, I found that this gentleman also frequented such establishments as 'Rick's Cabaret' and 'Flashdancers'. Using websites like Spokeo and Facebook, I was also able to find out his property value, ethnicity, relationship status, court records, and even a profile picture![10]

This example of taxi data is representative of the dangers of data that is made public. By simply releasing a dataset to the public, the privacy, and even safety, of an individual can be highly compromised; for example, using the taxi data, a thief could track the daily movements of an individual and then know when that person is away from home based on changes in these daily movements that they have observed.

People provide their data to businesses knowing, or at least hoping, that the business will keep their information secure and private in order to maintain their anonymity and safety. In the case of the NYC taxi data, by getting into a taxi, Bradley Cooper, for example, was automatically giving information about his personal life, including where he was going and how much money he would tip, to someone else. Assumedly, it did not occur to Bradley Cooper, as well as the rest of the general population who took taxis in New York City, that their data could be misused in a way that would compromise their privacy. If this thought had occurred to the general public, it can be assumed that the men who frequent Larry Flynt's Hustler Club, for example, would be more careful about traveling to and from the club, knowing that there was a possibility for their activities to be exposed simply by using the New York City taxi system. When it comes to personal data, however, people are surprisingly not

so careful and often provide digital data to the public willingly, for anyone and everyone to see.

Venmo is a mobile payment service owned by PayPal. On its website it is described as follows: "Venmo allows you to pay and request money from your friends. At its core, Venmo provides a social way to pay your friends when you owe them money and don't want to deal with cash." Venmo is most popular among millennials because of the social experience that it brings to splitting payments with others. In an interview with Matthew Bishop of The Economist, PayPal CEO Dan Schulman said the following:

> Venmo users open their app four or five times a week, but they only do transactions a couple times a week. But they're always looking at the feed to see what did you buy, what icons did you put on your feed, why did you go and buy that? So the secret sauce of Venmo is that one, it made it simple and easy, but two, it tied into your social network so that sharing payments became an experience and a sharing of part of what your life is.[11]

Although there is an option to make your Venmo transactions private, the default setting is for all transactions to be public, and most people, either knowingly or unknowingly, leave it this way. While payment transactions used to be just about giving money to someone you owe and receiving the money that you are owed, it has now turned into a social experience, a part of social media. In its description on the app store, Venmo is advertised as a way to split the bill at a meal or settle up for concert tickets with friends, but it is also advertised as a way to send money for purely social purposes: "Send a penny to say hi, or 5 bucks for good luck." This social element of Venmo has led people to be extremely lax in the kind of data that they allow the public to see, giving out details about their lives that they might not otherwise have done because they do not realize the safety concerns with doing so.

The Venmo API (application programming interface) is public and can be accessed by anyone through their website. When visiting the site, a person can view all data of the latest public transactions on Venmo. One example of a data entry is as follow:

{"payment_id": 3201948462, "permalink": "/story/5e5c4f5f76ab3339b727dc0b", "via": "", "action_links": {}, "transactions": [{"**target**": {"username": "Jaycie-Williams1997", "picture": "https://s3.amazonaws.com/venmo/no-image.gif", "is_business": false, "name": "**Jaycie Williams**", "firstname": "Jaycie", "lastname": "Williams", "cancelled": false, "date_created": "2019-08-14T16:34:22", "external_id": "2810455990992896823", "id": "62589893"}}], "story_id": "5e5c4f5f76ab3339b727dc0b", "comments": [], "updated_time": "2020-03-02T00:12:15Z", "**audience": "public**", "**actor**": {"username": "Brooke-Bondurant-2", "picture": "https://pics.venmo.com/3feff9e2-7483-49a9-9028-1dc52dcf1300?width=100&height=100&photoVersion=1", "is_business": false, "name": "**Brooke Bondurant**", "firstname": "Brooke", "lastname": "Bondurant", "cancelled": false, "date_created": "2020-02-28T15:46:47", "external_id": "2953937636294656511", "id": "74999745"}, **"created_time": "2020-03-02T00:12:15Z"**, "mentions": [], **"message": "Out to eat"**, "type": "payment", "likes": {"count": 0, "data": []}}

By simply visiting the Venmo API site, it is public knowledge that Jaycie Williams paid Brooke Bondurant because they went out to eat together on March 2nd.

A privacy advocate and designer named Hang Do Thi Duc created a project called Public By Default where she aims to showcase just how much data Venmo users release about themselves, and how much others can learn from this data. Public By Default is a website that uses Venmo's API to trace the spending habits, and therefore lives, of five 'unsuspecting humans'. On the site she provides detailed explorations of the lives of five different people, all taken from just their Venmo transactions. In one such case, she looks at the lives of a couple who frequently send each other money on Venmo. From their transactions she learns that they are from Orange County, CA, they own a pet which they take to the vet, and a car which they fuel every two weeks, usually at Chevron. They eat pizza very often, their favorite being from Shakey's, and they also like to eat German and Asian food. They buy most of their groceries at Walmart and, based on eight transactions that include the term SDG&E, they most likely rely on San Diego Gas & Electric for their electricity.[12]

With this information about this specific couple, a pizza store in the area might target this couple in their advertising since they clearly like pizza so much, or a pet store might target the couple in order to sell them pet-related items. These types of data usages, while invasive, are not necessarily harmful to the couple from California. Taxi data that reveals exactly when a person takes a cab from New York City to JFK airport, for example, seems much more detrimental, because, as mentioned, this kind of data can reveal that a person is away from home and offer an opportunity for thievery. In actuality, this can be applied to Venmo data as well. If, for example, the couple in California exchanges payments for the vet every week at a certain time, a thief can infer that perhaps no one is present in their home at this time every week, and then use this opportunity to break into their house.

Dan Salmon, a masters graduate from Minnesota State University who specializes in information security, explores another type of danger that accompanies giving away personal data on Venmo. Salmon describes how easy 'spearphishing' becomes with all of the available Venmo data. Spearphising is "an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer."[13] Salmon provides an example of such spearphising that could happen with Venmo:

> An attacker could easily find a list of the people that their target most frequently interacts with, as well as that person's common spending habits. For example, if Andy frequently interacts with Shannon to pay for concert tickets, an attacker could craft a highly believable phishing message for Andy that looks like Shannon is sharing information about a concert with him and that he should log in to his Ticketmaster account to view it.[14]

In the case of Do Thi Duc's project, the couple from California could be targeted by phishers in various ways; for example, in their Venmo transactions, "Chicago Ribs" appears five times, which Do Thi Duc says might be a reference to the restaurant Chicago for Ribs which is located

in three cities in California. Seeing this, a phisher might compose an e-mail to the couple telling them that they have been selected for a free meal at Chicago for Ribs, something that the phisher knows the couple would probably be interested in based on their eight visits there, when in reality, the e-mail is malicious and dangerous.

After learning of the various dangers of public data, a person might become wary enough that they are more careful to keep their data private; they will make their Venmo and other social media accounts private and be more conscious of all data that they allow others to collect about themselves on various websites and in various apps. A person might even be careful to only provide personal or sensitive data to another when they are certain that it is being kept private and not going to be used for advertising or other social purposes. Even the people most cautious about the type of data that they release to others, however, sometimes cannot avoid doing so, but they do so under the assumption that this data will be kept strictly private. For example, when a person books a hotel room there is no way to avoid providing personal information such as your name, credit card number, and sometimes even passport number, but people do so assuming that this information will stay within hotel records. A major problem of online data collection and storage is that online records, such as these hotel records, are subject to breach.

***b. Dangers of Privately Held Data***

Before data was collected online, everything was done on paper. Hospital records, hotel records, government records, and more, were all kept on paper. Therefore, there was no concern about personal consumer data falling into the wrong hands because it was kept locked away inside the establishment. With online data collection and storage, however, this is not always possible. Hackers often find ways to infiltrate an establishment's online systems and records in order to steal information.

On September 8, 2018, a suspicious attempt to access the internal guest reservation database for Marriot's Starwood hotel brands, which include the Westin, Sheraton, St. Regis, and W hotels, prompted an investigation into the network that revealed a serious network compromise in the Starwood system from four years earlier. Testimony from Arne Sorenson, President and CEO of Marriot International, that was given before the Senate Committee on Homeland Security and Government Affairs on March 7, 2019, outlines the events that occurred during and after the discovery of this security breach. The suspicious alert came about when Accenture, who managed the Starwood Guest Reservation Database, noticed an alert from their security product that indicated that a query was run on an administrator's account to return the count of rows from a table in the guest reservation database. After looking into this, they learned that the individual whose credentials were used on the administrator's account had not actually made such a query; through further investigation, Marriot discovered a Remote Access Trojan ("RAT"), which is a form of malware that allows an attacker to gain access to, or even control over, a computer. The attackers were so diligent, however, that it took a few weeks before the investigation experts and the FBI could even find evidence that the attackers had gained access to guest data in the Starwood database. Investigators finally found two compressed, encrypted files that had been removed from the Starwood network, and after six days they were able to decrypt them. They found that one of these files contained an export of a table containing guest data and the other file contained an export of a table containing guests' passport information. It was soon discovered that the attackers likely created copies of various other data tables from the Starwood system as well, but the specifics of those tables could not be found.

Although Marriot cannot say definitively how many peoples' information was compromised in this breach due to the likelihood of duplicates in the data, they did say that the

number of guest records that were stolen reaches up to 383 million. Marriot revealed that the incident involved 24 million passport numbers and 9.1 million credit card numbers. Although many of these passport numbers and credit card numbers were encrypted, they have no evidence as to whether or not the attackers had access to the necessary encryption keys needed for decryption. Regardless, at least 5.25 million passport numbers were found to be unencrypted.

Because of laws about an individual's 'right to know', Marriot provided a public notice of the incident via a press release and also created a website to provide information and updates about the incident to those who were affected. Marriot also created a process whereby customers of Marriot could ask what information about them, if any, was involved in the data breach.

As part of the testimony from Sorenson, he also outlined how Marriot planned to improve security and data privacy going forward. In addition to no longer using the compromised guest reservation database, and instead migrating all reservations into a secure database, he noted that Marriot would remove all malware and engage in IP whitelisting, which is the limiting of access only to trusted users and IP addresses, among other precautions.[15]

The effects of such a data breach are broad; millions of consumers had their data, which they had hoped would be kept strictly private, stolen. There are many possible ways that an attacker could negatively use sensitive information such as credit card and passport information. Theft of consumer data is often attributed to criminals hoping to make use of stolen credit card numbers, but the Marriot data breach went in a completely different, and perhaps even more serious, direction. In an article from December 11, 2018, the New York Times reported that the cyberattack on Marriot was part of "a Chinese intelligence-gathering effort." The Times reported that the hackers are suspected to have been working for China's

civilian spy agency, the Ministry of State Security. These suspicions emerged because firms who were brought in to assess the Marriot situation noted that the computer code and patterns used in the breach were reminiscent of other Chinese operations. The attack on Marriot was not an attempt to gain credit card information, as attacks on personal information such as this usually are, but rather, it was likely an effort to gain much more serious data. Lisa Monaco, a former homeland security adviser under Barack Obama, explained that Chinese attackers might pursue passport information because such information "would be particularly valuable in tracking who is crossing borders and what they look like, among other key data."[16] The Washington Post also explained how the information taken from Marriot might be valuable to a foreign intelligence agency. The Washington Post reported that the information could be used to "track movements of diplomats, spies, military personnel, business executives, and journalists… Armed with a rich array of personal data, an intelligence agency can also tailor an approach to a person to see whether the individual can be recruited as a spy or blackmailed for information. The passport data, which is not often collected in data breaches, probably was a particularly valuable find for the hackers."[17] Another clue that indicates that the stolen data was taken by a foreign agency rather than as a normal criminal act is that none of the data was found to be for sale online. Usually with criminal data breaches, the criminals create the attack in order to profit off of what they stole. In this case, however, whoever stole the data took it for their own purposes about which professional investigators can only speculate.

Booking a hotel room is commonplace. The average person would probably hope that when they provide personal data to a hotel, it will be held privately and securely. As important as it is for this type of data to be kept secure in order to preserve the privacy of individuals, it is perhaps even more essential that this privacy is maintained when government officials and their travel data are concerned. This type of data is extremely sensitive because it can reveal

deep insights into the lives and actions of government and military personnel. The Marriot case is an example of an enormous issue that emerges with online data collection and the extent of an individual's privacy that it can violate. Even when a person is most cautious about what kind of data they release and to whom they release it, sometimes, as in the case of booking a hotel room, it is unavoidable. This becomes a problem when the entity that is collecting that data allows for the possibility of a breach to take place. As mentioned, after the Marriot data breach, they changed their database and put many new precautions and safety features into place. If these safety features had been in place to begin with, perhaps the data breach might not have happened, and the privacy of over 300 million individuals might not have been violated.

## V. Is There Ever Reason to Invade Digital Privacy?

Hotel databases are just one example of data that individuals release under the expectation that it will remain private. Another example of digital data that is held privately is the data associated with electronic smart speakers and home assistants, such as a Google Home or Amazon Echo. In a letter written by Brian Huseman, vice president of public policy at Amazon, to Senator Christopher A. Coons, he describes how Amazon Echo works:

> [W]e designed Echo devices and Alexa to use on-device "keyword spotting" technology to detect when a customer intends to interact with Alexa; to use visual and audible signals to clearly indicate to customers when audio is being recorded for streaming to the cloud; to continually attempt to determine when a customer's request to Alexa has ended so we can minimize the amount of audio we stream to the cloud; to allow customers to see, hear, and delete the audio that was streamed to the cloud; and to let customers control when their Echo device's microphone is enabled through a microphone on/off button. We use the customer data we collect to provide the Alexa service and improve the customer experience, and our customers know that their personal information is safe with us.[18]

When a person purchases an Amazon Echo, they do so under the assumption that all data that is recorded inside their house will remain safe and is only used by Amazon in order to improve customer experience. Amazon uses Alexa data to improve customer experience by taking samples of customer voice recordings and having reviewers analyze the recordings to see if Alexa understood what the person asked and responded in the correct manner. Although data is only supposed to be stored when the device is activated, Amazon reviewers have noticed that sometimes Alexa begins recording mistakenly, without the correct prompt. One person even said that the reviewers sometimes transcribe as many as "100 recordings a day when Alexa receives no wake command or is triggered by accident."[19] Regardless, even when data is mistakenly recorded, Amazon has indicated that "customers know that their personal information is safe with us." Even though Alexa might pick up information without the person wanting it, Amazon is still committed to the fact that the individual has the right to see, hear, and delete this data, and they will not exploit the data.

An interesting question that arises with Alexa data, and, more generally, with any data that is promised to be held 'safe', as Amazon said in relation to their Echo device, is if there is ever a time where this promise can be bypassed and data that was supposed to be held private is permitted to be released. A serious implication of this is in the case of a criminal investigation.

Oftentimes in criminal investigations, digital data is used as evidence. When this digital data is public, using the data might not be a big problem. For example, in 2011, there was a personal injury lawsuit called Largent v. Reed in which plaintiffs Keith and Jessica Largent were in a car accident and claimed that they suffered 'serious and permanent physical and mental injuries, pain, and suffering'. The defense, however, claimed that Jennifer Largent's Facebook account, which had been public since January 2011, indicated that 'Largent had

posted several photographs that show her enjoying life with her family and a status update about going to the gym'. Because of this information that Largent publicly posted, the court ultimately ordered that Largent must turn over her Facebook username and password, thereby allowing the defense to view all posts that might be viable as evidence. The defense was given access to this data because the material sought on the Facebook page was proven to be relevant, and, furthermore, there is no reasonable expectation of privacy in material that is posted on a social network.[20]

In the Largent v. Reed case, Jennifer Largent was forced to surrender her Facebook username and password because she posted this information on a social networking site, and therefore it was not privileged information. With this logic, that the Facebook data was viable as evidence because it was on a public site and therefore not protected under privileged information laws, one might think that for a device such as Amazon Echo, in which data is not given by individuals to the public, such data should not be allowed to use in a court of law.

In 2015, a man named Victor Collins was found dead in the Arkansas home of his friend James Bates. After finding an Amazon Echo device in the home, prosecutors asked Amazon to turn over recordings from Bates's home; Amazon, however, adamantly refused to do so. Amazon explained that providing recordings from the home of an individual would be a violation of protection of speech which is covered by the First Amendment. In Amazon's Motion to Quash Search Warrant, the invasive nature of such recordings is described:

> Once the Echo device detects the wake word, the Alexa Voice Service endeavors to respond to any ensuing voice communications detected in the user's home. Accordingly, searching Alexa's recordings is not the same as searching a drawer, a pocket, or a glove compartment. Like cell phones, such modern 'smart' electronic devices contain a multitude of data that can 'reveal much more in combination than any isolated record,' allowing those with access to it to reconstruct '[t]he sum of an individual's private life.'

While this commitment of Amazon to the privacy of their customers is on the one hand comforting, on the other hand, it can also be concerning that it is possible for there to be existing, yet unusable, evidence in a murder trial. Recognizing this, in the same motion to quash, Amazon outlined the only way that they would be willing to release Amazon recordings. Amazon stated that in requesting recordings, the government must show proof of both a 'compelling need' (for example, that other methods of obtaining evidence are not available) and a 'sufficient nexus' (a substantial relation between the information sought and the reason for which it is being sought), in order for the request to be fulfilled.[21]

With this information, purchasing a digital home assistant is a personal decision in which individuals must recognize that while Amazon is committed to keeping their data safe and private, a situation could occur in which the company is forced to release a person's private information. This issue of data privacy that emerges with the increasing popularity of the digital home assistant is one with serious implications that is representative of the increasing number of ways that an individual's personal data can be used as technology advances.

## VI. Privacy Issues in Jewish Law and Its Implications on Digital Privacy

Privacy is a topic which is discussed extensively in Jewish law, and there are a variety of laws pertaining to it. In *Bamidbar*, Bilaam blesses the Jewish people, and in his blessing, he says, "How fair are your tents, O Jacob, your dwellings, O Israel!"[22] Rashi on this *pasuk* quotes the *gemara* which states that Bilaam here was praising their tents because he saw that the openings of the tents did not face each other.[23] This notion of privacy between tents was something that caught his attention as being special, and this praiseworthy nature of privacy has made its way into practical Jewish law. For example, the Turei Zahav on the *Shulchan Aruch* says that a person may enter his friend's *sukkah* without permission, but only if he is

certain that the *sukkah* owner will not be there. If it is possible that the homeowner might be in his *sukkah*, then a person cannot enter the *sukkah* because we do not want the homeowner to be surprised when his friend sees what he is doing.[24] This *halacha* exists to protect the privacy of the individual, because privacy is something which is essential in living a normal life. In general, Judaim has various laws that are relevant when analyzing the concept of individual privacy. The laws of *hezek re'iya*, which include laws of *tzniut* and *lashon hara*, as well as the laws of *rechilus*, are all helpful in exploring Jewish law as it relates to digital privacy.

### *a. Hezek Re'iya*

Many *halachot* pertaining to privacy are outlined throughout the *Shulchan Aruch*. Rav Yosef Karo in the *Shulchan Aruch* explains the details pertaining to *hezek re'iya*, literally meaning 'damage of seeing', which is the concept of damage that is inflicted upon a person when his privacy is invaded. One such law in the *Shulchan Aruch*, which is elaborated upon by the Rama, states that you are only allowed to build a window that faces your neighbor's yard if they give you permission; however, even with this permission, you are not allowed to stand at your window and look or gaze into the yard of your neighbor because you might cause damage to him.[25] The implication is that the permission that your neighbor gives you to build your window is so that you can open it for sunlight or air, but they are not relinquishing their privacy. Accordingly, if you are to pass someone else's house and their window or door is open, the assumption is that they opened their door or window for sunlight or air, and not because they do not care about their privacy. The *halacha* therefore commands that if you are passing by someone's house, it is forbidden to look inside, even if their windows or doors are open.

The word '*hezek'*, meaning damage, in *hezek re'iya* implies that some type of damage is done when gazing upon another person, thereby invading their privacy. The Ramban says that the damage that is done to a person when you invade their privacy falls under three categories: *tzniut*, *lashon hara,* and *ayin hara*.[26] We will focus on the first two of these three categories.

***i. Tzniut***

The Ramban says that by watching something that a person intends to do in private, you violate that person's observance of the law of *tzniut*. Rabbi Maurice Lamm writes that *tzniut* means "modesty, simplicity, a touch of bashfulness, and reserve. But perhaps above these, it signifies privacy."[27] When you invade someone's privacy, their *tzniut* is taken from them because you are watching something that they intended to do modestly.

When it comes to social media, one might assume that this type of damage of *tzniut*, or seeing something that someone intends to do privately, might not apply, because by definition, social media is a website or application that "enables users to create and share content or participate in social networking"; the entire purpose of social media is to share content, something which, whether it is personal data or not, reveals details about the user in some way. In reality, however, problems of *tzniut* can still occur on social media. On Facebook, for example, users have a list of 'friends' with whom they share their content, and users have the option of making all of their Facebook activity private so that only their 'friends' can see what they do. While it seems that there is no issue of *tzniut* here, since the user specifically posts content in order for their Facebook friends to see, what happens if a person logs into his friend's Facebook account? Suddenly, this person now has access to the Facebook activity of hundreds of people for whom he was not given permission, and suddenly, the damage that falls under *tzniut* occurs, because the viewer sees content that the poster did not intend to share with him.

While oftentimes information that is shared online is by default public, perhaps it is important to take into consideration the audience that the person sharing is intending to share with.

With the amassed availability of online information and the popularity of social media, it has become easier and more common to engage in online 'stalking'. If someone wants to gain information about another person, they can simply type the name of the person into a search engine, and they will be provided with all web content that matches this person. When evaluating whether this practice of searching online for details of a person is permissible by Jewish law, one factor that might be essential to take into consideration is the intended audience for any information that you may find. As with Facebook, it might be necessary to consider whether or not the person about whom you are searching for information would want you to have access to this information. Despite the fact that this information is technically readily available to the public online, according to Jewish law, searching for this information about a person might violate the concept of *tzniut* in privacy. The fact that someone's window to their house is open does not permit you to look inside. Similarly, perhaps the fact that information about a person exists online does not permit you to look at it. Just because it is there, does not mean they want you to see it, especially when considering the fact that personal information is often published online by others, rather than by the individuals themselves.

### *ii. Lashon Hara*

Another type of damage that falls under *hezek re'iya* according to the Ramban is that when a person invades the privacy of another, they might come to speak *lashon hara*. In the *Chofetz Chaim*, Rabbi Yisrael Meir Kagan writes that *lashon hara* is the prohibition of speaking negatively about another person. When someone engages in online stalking, and therefore catches a glimpse into the private or personal life of another person, it is extremely possible that this will lead him to engage in *lashon hara* with his newfound information. It is

later written in the *Chofetz Chaim*, "If one revealed to his friend, in the presence of three, details of his occupation or trade or the like, things which, in general, are otherwise forbidden to repeat afterwards to another, lest this result in injury or pain to him – now, since he himself revealed it in the presence of three, it is evident that this is of no concern to him, even if it comes to be known in the end."[28] Rabbi Moshe Leib Halberstadt applies this law to the internet. He says that according to this teaching of the *Chofetz Chaim*, if a person were to publish information about himself on his own website, he implies that he does not mind if people know this information, and, therefore, as long as this information is not negative, this does not fall under the prohibition of *lashon hara*, and someone who views the website may share the information with others.[29]

This is in contrast to a case where the information the person publishes on his website about himself *is* negative, as well as to a case where negative information about a person exists online that he himself did not publish; in both of these cases, the act of sharing information that you find online *would* fall under the prohibition of *lashon hara*. One issue that Jewish law might present in relation to online data is that with so much information available online, even though this is technically public information, it is almost inevitable that an individual will find negative information about another person and ultimately share it; for example, New York City publicized their taxi data, and suddenly Anthony Tockar, the graduate student from Northwestern, ran some simple queries on the data and revealed to the public the tipping habits of certain celebrities. He discovered that Bradley Cooper and Jessica Alba did not tip their taxi drivers, and revealed this arguably negative information to the public, thereby constituting *lashon hara*.

***b. Rechilus***

Even if a person does not come to share the negative information that they find with anyone else, there is another type of prohibited speech which might prevent one from seeking out information, despite the fact that the person might avoid speaking *lashon hara*. In *Vayikra*, the *pasuk* states, "Do not go as a *rachil* among your people."[30] Rashi explains on this *pasuk* that the Hebrew word מרגל means 'to spy', and because letters for which the pronunciations are of the same place in the organs of speech may be interchanged, the letter 'כ' can be interchanged with the letter 'ג'. Rashi therefore equates the word רגל with the word רכל to explain that *rachil* in this *pasuk* means a spy. The *pasuk* is therefore telling us not to go around 'spying' and spreading negative information.[31] The Rambam takes this a step further and defines a *rachil* as a person who carries information and goes from person to person saying, 'this is what so-and-so said', or 'this is what I heard about this person', even if it is true.[32] The Rambam does not limit *rechilus* to negative information, as Rashi does, rather, he says it includes spreading *any* kind of information about another person. Taking this another step further, Rav Yaakov Chagiz writes about a *rachil*: "What difference does it make if he goes about as a spy to reveal something to someone else or to himself?"[33] Rav Chagiz here does not limit *rechilus* to spreading information, rather he explains that there is actually no difference between revealing information that you find to someone else and revealing it to yourself- he says that both constitute *rechilus*.

While Anthony Tockar avoided the prohibition of *lashon hara* by not releasing in his article the names of the men whom he tracked as frequent customers of Larry Flynt's Hustler Club, he wrote in his article that he was able to conduct a simple search for an address that is a frequent drop off location from the club, and with very little effort, he discovered private information about a person. Similarly, when Hang Do Thi Duc created her Public By Default website to illustrate the dangers of public Venmo data, although she did not release to the

public the names of the people whose lives she tracked based on their spending habits, thereby avoiding *lashon hara*, nevertheless, she investigated personal details of the lives of specific individuals and collected information from their online Venmo data. Perhaps Rav Chagiz would say that Tockar's and Do Thi Duc's entire projects where they sought out information about specific people on the internet constitutes the prohibition that is *rechilus*.

This is an alarming teaching by Rav Chagiz, because he forces us to consider whether there is any kind of online information, or really information in general, that is permissible to seek out. Perhaps by seeking out information, for example by conducting even a simple Google search about someone, a person is becoming a *rachil*, one who reveals information to himself.

If we conclude that Jewish law prohibits the act of seeking out personal data about individuals on the internet, an interesting *halachic* question that emerges is what one should do if searching for such information is part of their job. For example, if a Jewish person works in the human resources department of a company, and their job is to hire new people, is this employee allowed to 'stalk' a job applicant on the internet in the hopes of finding more information about them to determine if they would be suitable for the job? Something that might help in answering this question is the question of if there is ever a situation in which Jewish law permits violating another person's privacy.

### *c. Extenuating Circumstances*

Privacy is extremely important in Jewish law, however, there are numerous sources which indicate that the laws protecting the privacy of an individual may be broken in extenuating circumstances. The Ibn Ezra writes, "if a secret was revealed to you and you can save someone from death by revealing it to him – if you do not reveal it, you are like a murderer."[34] The Ibn Ezra here notes that privacy can be broken in order to save another person from death. Later rabbis have used this ruling of the Ibn Ezra in their own, more modern

rulings. Rav Moshe Shternbuch ruled that if a doctor determines that a patient is unfit to drive, he may break doctor-patient confidentiality rules by informing appropriate authorities for the sake of public safety. Similarly, Rav Ovadia Yosef ruled that a doctor must inform the authorities if he determines that a patient with epilepsy is unfit to drive, in order to maintain public safety as well.[35] In the Bates/Collins Arkansas murder case, while Amazon demanded proof of both a compelling need and sufficient nexus before releasing private Alexa data that might be relevant to the murder, Jewish law seems to indicate that the private Alexa data *must* be investigated if there is a possibility that it will lead to the apprehension of a murderer who will otherwise pose a threat to society.

Based on the many sources which indicate that one is required to share another person's secret in order to maintain safety, it is reasonable to conclude that all the more so, one should be required to share information that is *not* a secret for the sake of safety. Particularly, personal information that exists on the internet, while possibly private, is not considered secret information, as it can be found by anyone. Jewish law might, therefore, suggest that it is permissible, and perhaps even required, to use this kind of non-secretive information for the sake of protecting the safety of others.

In the HR job example, when someone applies for a job, they usually just send in their resume. While a resume provides general information about the career of the individual, it usually does not provide personal information; a company, however, probably wants to make sure that the applicant is an ordinary, safe person before bringing them into the company. One way the company can help to ensure this is by searching for information about the applicant on the internet. By searching for this person on Google, the HR employee might find valuable information about the applicant. If, when 'stalking' the applicant, the employee is able to find evidence that the applicant was involved in a crime, for example, this quick Google search

might have saved the company from hiring someone who might be dangerous and might have posed a threat to the rest of the company had they been hired. In general, it might be important for individuals to evaluate whether there is some kind of potential danger involved when deciding if they may partake in a job that compromises the privacy of another person.

## VII. Conclusion

The issues involving online data are extensive and complex, as well as everchanging. Even just thirty years ago, most of the issues outlined in this essay did not exist as they do now, and they will likely be extremely different to how they are now in another thirty years. It is important to recognize the various issues that exist because by doing so, we will have a better chance of anticipating, and therefore managing, the ongoing privacy issues that have been escalating in creativity and severity with increasing amounts of online data. Based on the current trajectory of data privacy issues that have emerged, it seems inevitable that these issues will only grow larger and worsen as technology advances and online data is collected even more. There is one tactic, however, that will not solve privacy issues completely, but can definitely mitigate the issues so that at least some amount of privacy is maintained.

As mentioned earlier, *tzniut* is the concept of modesty in Jewish law. In the *Midrash Tanchuma* it is written that the first set of *luchot* (tablets) were shattered because they were given in public and were therefore dominated by an *ayin hara* (evil eye). It is then written in the *midrash* that G-d said to Moshe, "There is nothing more beautiful than modesty, as it is said: And what does G-d demand from you- but only to do justice and to love kindness and to walk modestly."[36] In this situation, it is evident that being public was equated with immodesty.

The possible link between looking into a person's house and looking for information about them online, as both being a violation of the *tzniut* of the individual, was explained

earlier. By seeking out information about a person, whether it is via their open windows or via data available on the internet, you detract from their observance of the requirement to be modest. It is worth exploring an alternate application of *tzniut* to the situation; if a person abides by the true meaning of the laws of modesty and is careful to lead a private lifestyle, free from ostentation and extravagance, many issues of online data privacy can be avoided altogether. The opinion of the Ramban that was quoted earlier, about the types of damages that are inflicted upon a person when their privacy is invaded, explains further that even if the 'damaged' relinquishes his rights to privacy, it is still forbidden for the 'damager' to cause damage to him by knowingly looking at him. Even if the person does not care if you see him, it is still forbidden. The Ramban then says that no person can be sufficiently careful about this, and one would need to have his eyes closed at all times in order to avoid this transgression. In conclusion, the Ramban says, "We are compelled to say to him [the damaged]: close your window and you will not sin constantly." If a person just keeps their window closed, the issue of privacy in their home is simply avoided altogether.

This can be applied to online privacy as well. One of the most popular forums for online data collection is social media. According to the Pew Research Center, over 72% of the public uses some type of social media.[37] Every minute of the day, 527,760 photos are sent on Snapchat, 456,000 tweets are sent on Twitter, and 46,740 photos are posted on Instagram.[38] Although social media has become so popular and widely accepted in the secular would, if a person were to refrain from indulging in social media, which encourages sharing personal information online, and instead were to look towards the guidelines of *tzniut* set forth in Jewish law, which discourages sharing personal information and encourages living in a more modest and private manner, many issues of privacy involving online data could be avoided. Someone who leads a truly *tzniut* lifestyle will not be posting pictures of their lavish vacation on

Facebook, even if it is just for their 'friends' to see, and they will be sure to create a private Venmo account where they are not constantly sharing their activities and spending habits with the public. Conducting one's behavior in a modest manner ultimately leads to less information about that person being available to others, which in turn leads to less data privacy issues. If individuals take care to 'close their windows', as the Ramban says, and act modestly with the details of their lives, the problems that result from online data privacy would surely be diminished.

## VIII. References


[1] "Apple Pay Overtakes Starbucks as Top Mobile Payment App in the US." *EMarketer*, 23 Oct. 2019, www.emarketer.com/content/apple-pay-overtakes-starbucks-as-top-mobile-payment-app-in-the-us.

[2] Marr, Bernard. "Starbucks: Using Big Data, Analytics And Artificial Intelligence To Boost Performance." *Forbes*, Forbes Magazine, 31 May 2018, www.forbes.com/sites/bernardmarr/2018/05/28/starbucks-using-big-data-analytics-and-artificial-intelligence-to-boost-performance/#21748b6865cd.

[3] Streitfeld, David. "'Black Mirror' Gives Power to the People." *The New York Times*, The New York Times, 28 Dec. 2018, www.nytimes.com/2018/12/28/arts/television/black-mirror-netflix-interactive.html.

[4] Sharp, Tim. "Right to Privacy: Constitutional Rights & Privacy Laws." *LiveScience*, Purch, 12 June 2013, www.livescience.com/37398-right-to-privacy.html.

[5] The Editors of Encyclopaedia Britannica. "Rights of Privacy." *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 26 Feb. 2020, www.britannica.com/topic/rights-of-privacy.

[6] "Assembly Bill No. 375." *California Legislative Information*, 29 June 2018, leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[7] Wolford, Ben. "What Is GDPR, the EU's New Data Protection Law?" *GDPR.eu*, 13 Feb. 2019, gdpr.eu/what-is-gdpr/.

[8] "The Personal Information Protection and Electronic Documents Act (PIPEDA)." *Office of the Privacy Commissioner of Canada*, 4 Sept. 2019, www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

[9] "New York State Education Department FOIL Requests." *New York State Education Department*, www.nysed.gov/new-york-state-education-department-foil-requests.

[10] Tockar, Anthony. *Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset*. 20 Aug. 2015, atockar.wordpress.com/projects/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/.

[11] "PayPal CEO Dan Schulman on the 'Venmo Line' and the Fact That Cash Will Never Die." *Business Insider Australia*, Business Insider Australia, 22 Dec. 2015, www.businessinsider.com.au/paypal-ceo-dan-schulman-interview-2015-12.

[12] Do Thi Duc, Hang. "PUBLIC BY DEFAULT." *Venmo Stories of 2017*, 2018, publicbydefault.fyi/.

[13] "What Is Spear Phishing? - Definition." *Usa.kaspersky.com*, usa.kaspersky.com/resource-center/definitions/spear-phishing.

[14] Salmon, Dan. "I Scraped Millions of Venmo Payments. Your Data Is at Risk." *Wired*, Conde Nast, 26 June 2019, www.wired.com/story/i-scraped-millions-of-venmo-payments-your-data-is-at-risk/.

[15]*Testimony of Arne Sorenson, President & CEO, Marriott International Before the Senate Committee on Homeland Security & Governmental Affairs Permanent Subcommittee on Investigations*. 2019, www.hsgac.senate.gov/imo/media/doc/Soresnson%20Testimony.pdf.

[16] Sanger, David E., et al. "Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing." *New York Times*, 11 Dec. 2018, www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.

[17] "U.S. Investigators Point to China in Marriott Hack Affecting 500 Million Guests." *Washington Post*, 2018, www.washingtonpost.com/technology/2018/12/12/us-investigators-point-china-marriott-hack-affecting-million-travelers/.

[18]Huseman, Brian. Received by Senator Christopher A. Coons, 28 June 2019, www.coons.senate.gov/imo/media/doc/Amazon%20Senator%20Coons__Response%20Letter__6.28.19%5B3%5D.pdf.

[19] Day, Matt, et al. "Amazon Workers Are Listening to What You Tell Alexa." *Bloomberg.com*, Bloomberg, 10 Apr. 2019, www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.

[20] Pennsylvania Court. *Largent v. Reed*. 8 Nov. 2011, www.theemployerhandbook.com/files/2015/01/Largent.pdf.

[21] The Circuit Court of Benton County, Arkansas. *State of Arkansas v. James A. Bates*. 17 Feb. 2017, www.documentcloud.org/documents/3473799-Alexa.html.

[22] Bamidbar 24:5

[23] Talmud Bavli, Bava Basra 60a

[24] Turei Zahav 637:4

[25] Shulchan Arukh, Chosen Mishpat 154,

[26] Chidushei Ramban, Bava Basra 59a

[27] Lamm, Rabbi Maurice. "Modesty (Tzniut)." *My Jewish Learning*, www.myjewishlearning.com/article/modesty-tzniut/.

[28] Chofetz Chaim 2:13

[29] Halberstadt, Rabbi Moshe Leib. "Lashon Hara/Internet." *Yeshiva*, 18 Aug. 2013, www.yeshiva.co/ask/6488.

[30] Vayikra 19:16

[31] Rashi, Vayikra 19:16

[32] Mishneh Torah, Hilchot Deot 7:2

[33] Halachos Ketanos 1:276

[34] Ibn Ezra, Shemot 20:13

[35] Lichtenstein, Rabbi Dovid. "Facebook, Cambridge Analytica and the Right to Privacy: A Halachic Overview." 20 May 2018.

[36] Micah 6:8

[37] "Demographics of Social Media Users and Adoption in the United States." *Pew Research Center: Internet, Science & Technology*, Pew Research Center, 12 June 2019, www.pewresearch.org/internet/fact-sheet/social-media/.

[38] Marr, Bernard. "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read." *Bernard Marr*, www.bernardmarr.com/default.asp?contentID=1438.