The Internet Privacy Paradox: understanding the role online services, governments, and businesses have on the privacy behavior of individuals

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Phillip Phan
Spring, 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature Phillip Phan Date _05/04/21__
Phillip Phan

Approved H Rogers Date _05/04/21__
Hannah Rogers, Department of Engineering and Society

Abstract

Studies have shown that a majority of Americans believe that it is important to be able to control who can obtain information about them, but only a small minority report taking action to protect their privacy. This gap between consumer's attitudes and actions is known as the privacy paradox. Through Actor Network Theory (ANT), an analysis of consumers' relationships with online services, companies, and the U.S. government showed how these relationships resulted in a systematic power dynamic that favors the U.S. government and companies over consumers, and eroded consumers' confidence in their data being protected from third parties. These factors resulted in the prevalence of the privacy paradox among consumers. The structural power imbalance in U.S. society limits the amount of influence that consumers have to change existing privacy regulations and protect their privacy. To combat the effects of the privacy paradox, consumers need to work together through consumer activist groups to help enact new privacy legislation that ensures consumers' privacy is protected.

The Internet Privacy Paradox: Understanding the role Online Services, Governments, and Businesses have on the Privacy Behavior of Individuals

"Alexa, turn off the lights." The lightbulbs in the room turn off, controlled by the Amazon Alexa assistant. The rise of online services such as IoT devices, over the past two decades has resulted in a wider range of convenience for consumers as online services enable consumers to turn on light bulbs with a spoken command, for example. This convenience, however, comes at a hidden cost as consumer data from using online services is sold to advertisers who use this data to show targeted advertisements to influence consumers to purchase a product or service. Aside from changing the shopping habits of consumers, advertisers can use consumer data to influence consumers' behavior by inducing consumers to believe disinformation, which is exemplified by the Cambridge Analytica data scandal in 2018 (Rosenberg et al., 2018). The collected data from online services can potentially be used for more malicious causes in the future as shown by how China has weaponized online data to curb dissent (Mitchell & Diamond, 2018). These scenarios emphasize the need for consumers to use products that minimize the collection of personal data and advocate for strong privacy laws to curtail the amount of data companies and governments collect on consumers. However, only 9% of American adults reported taking action to avoid having their online activities tracked despite 93% of respondents believing that it is important to be able to control who can obtain information about them (Madden & Rainie, 2015). This disconnect between consumers' attitudes and actions is also known as the privacy paradox (Williams et al., 2015).

While the term, "privacy paradox," was first coined in 1998, the current usage of the privacy paradox as a term to describe the gap between consumers' privacy attitudes and actions was first defined in 2000 (Bedrick et al., 1998; Sweat, 2000). Due to the contradictory nature of

the privacy paradox and concerns from privacy advocates about the erosion of digital privacy, researchers conceptualized the privacy paradox to succinctly describe how consumers give up their privacy to be able to use an online service. As online services have rapidly multiplied over the past two decades since the privacy paradox was first coined, scholars have formulated various hypotheses to describe why the privacy paradox is widespread among consumers. Understanding why there is a gap between consumers' beliefs and their actions is crucial to ensure that consumers' personal data is not being misused by either businesses or governments.

The number of internet-connected devices per capita is expected to rise from an average of 8.2 devices in 2018 to 13.6 in 2023, representing an increase of 66% ("Cisco Annual Internet Report (2018–2023) White Paper," 2018). This growth of new internet-connected devices exacerbates the privacy paradox as users become accustomed to countless devices that collect data about every facet of a consumer's life. Actor Network Theory (ANT) will be used to analyze how the proliferation of online services over the past decade, and the shared interests between governments and businesses resulted in a power imbalance that favors governments and companies over consumers. These factors contribute to the prevalence of the privacy paradox among consumers.

Consumers and Privacy

Consumers are the individuals who use online products or services that collect information about themselves. As they use online services and products, consumers want to minimize the amount of data that is collected about themselves to maximize their individual privacy. Protecting one's privacy enables consumers to protect themselves from unwarranted interference in their lives and empowers consumers to have the freedom to choose how they want to act in society. The U.S. Supreme Court found that individuals are entitled to an implied

"right to privacy" in *Griswold v. Connecticut* ("Griswold v. Connecticut," n.d.). While the ruling for *Griswold* found a right for privacy in the specific case of married couples purchasing contraceptives, the idea of an individual's right to privacy was gradually expanded over the past century through other court cases ("Privacy," n.d.). As the internet recently exploded in popularity, the privacy of consumers no longer fits neatly into existing judicial precedents. However, recent court cases like *Carpenter v. United States* are helping to establish a constitutional baseline for how much of an individual's online data is protected ("Carpenter v. United States," n.d). These court cases highlight how the absence of comprehensive data privacy legislation in the U.S. is forcing U.S. courts to handle how an individual's online data is used by the U.S. governments and companies when it should be the role of the U.S. government to regulate consumers' privacy.

Legislation passed by other governments like the EU's General Protection Regulation (GDPR) reinforce how privacy is a key human right that is necessary to protect even if data privacy is not as strongly protected in the U.S (Wolford, 2018). To continue protecting their online privacy, U.S. consumers need to use privacy-focused online services and advocate for more stringent data collection laws like the GDPR. These actions will enshrine privacy as a right for U.S. consumers and ensure that consumers' interests are protected from other third parties.

Businesses

As Americans gained access to the internet over the past two decades, internet companies that provide free services proliferated across the internet. Instead of charging subscription fees to use their services, many companies recognized that consumer data is the most valuable resource they can obtain from consumers because they can influence and predict the behavior of consumers using this information. Companies, like Google and Facebook, analyze consumers'

behavior to show advertisements that influence what consumers might purchase. Showing advertisements to a target demographic is highly lucrative as Facebook had an advertising revenue of $69.66 billion and Google had an advertising revenue of $134.81 billion in 2019 (Clement, 2020a; Clement 2020b). Other companies incorporate consumer data to improve the performance of their products. For example, insurance companies use consumer data to optimize the pricing of insurance plans and minimize their risk exposure so that their expected revenue is maximized ("Big Data," 2020). For these companies, consumer data is inextricably tied to their business model and they will continue to develop new techniques to surreptitiously collect consumer data and improve the services they offer.

Governments

The U.S. government was formed to help protect the interest of their constituents, which include national security. There is a social contract between consumers and the U.S. government as consumers pay taxes, and in exchange, the U.S. government provides various services such as protecting individuals from harm and fostering economic growth. To maintain the relationship between consumers and the U.S. government, the U.S. government needs money to fund services for U.S. consumers and information to properly execute the services the U.S. government provides. For example, information encompasses intelligence reports on possible threats to U.S. citizens and data about the health of the U.S. economy (Adkins, 2020). Using this information, the U.S. government can take action to neutralize security threats and maintain the health of the U.S. economy, respectively. These examples show how the U.S. government needs a continuous flow of information to uphold their side of the social contract, and emphasizes the U.S. government's interest in obtaining more information. As the amount of data that consumers

generate is growing exponentially in the internet age, the U.S. government's interest in consumer data is growing proportionally at the cost of consumers' privacy.

These situations highlight the crossroads that consumer privacy is currently at since the U.S. government and companies both have an interest in consumer data. There are two possible paths that consumer data in the U.S. can undergo: either consumers will not have an expectation of privacy such as in China or consumer data will be vigorously protected by the U.S. government, which is the approach championed by the EU through the GDPR. To analyze the future of consumer privacy in the U.S. and the relationship between U.S. consumers, companies, and governments, a network analysis is used to map out the specific relationships between each actor. The relationship between companies and governments are examined first before analyzing each actor's relationship to consumers. Understanding the relationships between each actor through this network analysis is crucial to understanding how structural factors have affected consumers' privacy attitudes and exacerbated the privacy paradox.

Companies and Government

U.S. companies and the U.S. government have a strong relationship with each other as the U.S. government protects businesses' assets and intellectual property by enforcing various laws. These laws include preventing robberies and enforcing intellectual property laws, which enables businesses to fairly compete with each other to maximize their profits. In exchange, companies follow U.S. laws and pay taxes as part of their social contract with the U.S. government. Companies also must serve warrants that governments give to them as part of complying with U.S. laws, which involves handing over data about consumers to law enforcement agencies and intelligence agencies (Pagliery, 2017). With both actors following this

social contract, U.S. companies and the U.S. governments are able to accomplish their respective goals of earning money and protecting national security.

The relationship between the U.S. government and companies is not only limited to enforcing existing laws, but also in the process of creating new laws. Companies utilize lobbyists to lawfully influence the actions of politicians in the U.S. As a part of lobbying, companies cultivate relationships with congressional representatives and other key political figures by donating money to their political action committee (Paletz, 2016). In exchange, companies are subject to laxer laws that enable them to collect more data about consumers and maintain their continued success. The importance of lobbying is highlighted by how big tech companies such as Microsoft and Facebook each spent more than $10 million on federal lobbying in 2019 according to the Center for Responsive Politics ("Client Profile: Microsoft Corp.," 2020; Client Profile: "Facebook Inc.," 2020). The money that companies spend on lobbying results in favorable outcomes for these companies such as how Microsoft was able to revive their bid to acquire TikTok after calling two dozen lawmakers (Weise & McCabe, 2020). This scenario highlights the pervasiveness of lobbying in the U.S. government, and emphasizes the win-win relationship between companies and governments.

However, consumers are the social group that is negatively affected by lobbying as they lack the same spending power that companies have to influence lawmakers. Additionally, the laxer regulations that companies promote results in more data being collected from consumers, which results in these companies becoming more entrenched in society as they are able to use consumer data to continue improving their products and ensure their future success. As consumers wield significantly less influence over the creation of laws that regulate consumer data compared to tech companies, consumers feel disillusioned about the possibility of using

regulations to rein in tech companies' data collection. Consumers' disillusionment about creating new laws to regulate data collection is one of many factors that result in consumer inaction towards protecting their privacy.

Increasingly, anonymized consumer data is being used by companies and the U.S. government to help conduct beneficial research at a large scale. For example, data from individuals is used to help train machine learning models to improve early diagnosis of diseases from medical data and identify novel therapies (Alba, 2014; Myszczynska et al., 2020). Consumer data is also used to help improve the capabilities of speech-to-speech translation systems to allow individuals who speak different languages to communicate with each other (Jia & Weiss, 2019). In addition to the U.S. government's independent research labs, the U.S. government also partners with third-party companies to conduct research using anonymized consumer data. In this context, the U.S. government and companies' interests align as both parties seek to maximize the amount of useful consumer information that they can use for their research. However, the U.S. government also regulates how consumer data is collected and used by other groups. This situation highlights the conflicting role that the U.S. government has over consumer privacy as both a data collector and regulator of user data. Because of the U.S government's conflicting interests as a data collector and regulator, the U.S. government prioritizes national security and the interests of businesses at the expense of consumers' privacy, eroding consumers' confidence in their data being protected from third parties.

Companies and Consumers

When a consumer registers to use an online service like Facebook, the consumer is greeted with a terms of service that they have to sign and abide by if they wish to use the online service (Singer, 2018). Also known as a terms and conditions agreement or privacy policies,

these terms of service are often verbose, opaque and full of jargon that an average individual would not understand, especially due to the background knowledge that is required to understand them such as knowledge of how cookies are used in data collection. A study done by The New York Times found that the vast majority of privacy policies exceed the college reading level (Litman-Navarro, 2019). Because of how complex it is to understand these terms of services, consumers frequently skip reading them before signing the terms of service. Studies have shown that only 22% of American consumers always or often read the terms of service before signing one, and among American consumers who have ever read privacy policies before agreeing to the terms of service, only 22% of them have fully read through the terms and conditions before using an online service. Additionally, 59% of U.S. adults do not understand how companies use the data that is collected about themselves (Auxier et al., 2019). These studies reflect the information asymmetry between consumers and businesses as the businesses providing the online service use consumer data in ways that consumers cannot imagine, which is obscured by companies' inscrutable privacy policies.

In privacy policies, consumers are required to allow the company to collect information about themselves and are forced into mandatory arbitration clauses that prevent consumers from being heard in court if harmed by a service (Wilf-Townsend, 2019). Thus, the privacy of an individual can be compromised, and the individual would have limited options to seek recourse.

As online services proliferated in American society, the majority of Americans have obtained internet-connected devices like smartphones or laptops to use these online services. Internet-connected devices are key to navigating modern society as some actions such as applying to jobs can only be done online. The necessity of using online services in day to day life results in a power imbalance between the companies that provide the service and consumers who

have to use a company's service. For example, a consumer needs to provide their personal information to Facebook if the consumer wants to talk to a friend that is only on Facebook or a consumer needs to give their location data to Google Maps to accurately navigate the consumer to their destination. In these scenarios, consumers have to give up some of their personal data as part of the terms of service they signed to obtain a service of being able to contact a friend or reach a specific location. Additionally, the power companies hold over consumers is drastically increased if companies have minimal competition for the same online service. As consumers do not have alternatives if a company has a unique proprietary service or if there is collusion between multiple companies for a specific service, companies are able to set the terms to use their products and consumers have no choice but to accept them if they want to use a specific service.

Because of the systematic power imbalance that heavily favors a business over an individual consumer, businesses are able to dictate how they use gathered data with minimal resistance from consumers. This relationship between consumers and businesses contributes to how consumers feel helpless about taking action to protect their online privacy as regardless of what they do to protect their privacy, companies will still collect consumers' personal data. Additionally, if consumers try to work together and sue companies for violating their rights, forced arbitration clauses result in these challenges failing causing consumers to feel powerless. This feeling of powerlessness results in inaction among consumers to protect their privacy, contributing to the privacy paradox being pervasive among consumers.

Government and Consumers

In response to the September 11 attacks, the U.S. government prioritized "total information awareness" to prevent similar attacks from occurring again. To achieve the goal of

"total information awareness", Congress passed a number of bills to drastically increase U.S. national security such as the USA Patriot Act, which gave the federal government greater powers that includes monitoring telephone communications and e-mail (Lind, 2015). Because of the increased powers Congress granted to the federal government, the National Security Agency (NSA) established PRISM, a surveillance program that collected internet communication from U.S. companies, in 2007. PRISM is significant because it enables the NSA to obtain targeted communication from an individual without having to request them from service providers and without having to obtain individual court orders as long as there was reasonable suspicion that one of the parties was outside the U.S (Greenwald et al., 2013). This enables the NSA to collect data on a vast amount of Americans who communicate with individuals overseas even if they have not been accused of wrongdoing.

Additionally, secrecy over various government surveillance programs meant that there is no way for an independent third party to verify that the NSA was acting legally in its collection of data. Even if the NSA fully abided by the legislation that established PRISM by only collecting communications that involved a non-U.S. party, the data of countless American consumers would also have been incidentally collected and stored in huge databases. Within these huge databases, other government agencies can easily search for the communications of specific Americans all without ever seeking approval from a judge. Until these programs were leaked by Edward Snowden in 2013, Americans did not know that the government was surreptitiously collecting data about them (Greenwald, 2013). The federal government has an interest in keeping surveillance programs secretive as it prevents counter-measures from being developed and they would not be subject to restrictions that would limit their ability to stop future terrorist attacks and catch criminals.

U.S. government criticisms of data privacy laws, like the EU's GDPR, shows how the U.S. government wants to avoid restrictions on their surveillance capabilities as these data privacy laws shield cybercriminals from law enforcement agencies (Vinocur, 2020). The U.S. government also advocates for backdoors to be built into technology products such as WhatsApp and iPhones, which further emphasizes how governments prioritize accessing consumer data to enforce laws instead of protecting an individual's right to privacy ("International Statement: End-To-End Encryption and Public Safety", 2020). As the U.S. government and companies benefit from having access to more consumer data, their interests directly lie in conflict with consumers' interests who would want to protect their data. The prevalence of widespread surveillance programs combined with the U.S. government's insistence on having access to more consumer data is normalizing consumer data collection and molding consumers' privacy actions to accept invasive data collection from the U.S. government. By convincing consumers of the necessity for the U.S. government to collect consumer data, greater amounts of consumer data will be collected under the pretense of ensuring national security and consumer's attitudes towards privacy will irrevocably be affected.

Consumers and Online Products

For millions of people across the world, free online services have fundamentally changed the world in a variety of ways such as social media being used to connect countless individuals across the world. Before they use a specific service, consumers consider a wide range of factors such as the user interface and the privacy of an application. For many individuals, studies have shown that the usability, utility, and price of an application take precedence over any privacy concerns (Barth et al., 2019). The usability and utility of an application takes on many different forms such as better traffic-mapping algorithms for a navigation application or being able to see

algorithmically sorted reviews of nearby restaurants. Consumer preference for functionality over privacy highlights how consumers would rather give up some of their privacy instead of having a suboptimal experience with using a different online service. Similarly, unwillingness by consumers to pay for online services shows how the financial cost for using an online service overrides privacy concerns. Because of these factors, the popularity of free online services like Google can be explained despite the amount of data that is collected from each service. Services like Google and Facebook are free for consumers and they provide some form of measurable utility to their users. One possible explanation for why consumers prioritize these factors over privacy concerns is because consumers are unaware of the value of their data and the tradeoff that they make to use free online services. Consumers' consideration of other factors besides privacy concerns in choosing to use an online service and their ignorance regarding how their data is used shows how the privacy paradox is affected by factors that are not directly related to privacy.

The continued proliferation of new online services and products is a result of continued technological innovation and marketing by tech companies. The rise of IoT devices over the past five years, for example, highlights how companies' innovation is resulting in countless new online services that consumers can sign up for. IoT devices are able to collect consumer data through new vectors compared to traditional online services such as through one's voice data. Individuals' voice recordings are analyzed by researchers and QA testers to help improve the performance of IoT devices, raising privacy concerns from critics (Lynskey, 2019). As companies churn out new online products, the amount of data and the methods that they can use to collect this data will continue to increase, which is normalizing invasive data collection in society. The normalization of consumer data collection combined with repeated consumer data

breaches results in consumers feeling a loss of control over their data and contributes to consumers' weariness about protecting their privacy. Gradually, consumers became fatigued about protecting their privacy from companies and the U.S. government, resulting in the prevalence of the privacy paradox.

Despite the prevalence of the privacy paradox among consumers, there are countless activist groups such as the American Civil Liberties Union (ACLU) that are fighting to protect the privacy of American consumers. Activist groups protect the privacy of American consumers by encouraging consumers to switch to privacy-focused alternatives such as DuckDuckGo and by advocating for new privacy legislation to be passed like the EU's GDPR. Additionally, consumer groups can use the media to draw consumers' attention to the governments and companies that have egregious data collection policies. As a third party, activist groups act as a watchdog for consumers by counteracting the influence of companies and governments, which helps stymie the spread of the privacy paradox among consumers.

Conclusion

The analysis of consumers' relationships with online services, companies and the U.S. government shows how the power dynamics between each group affected the privacy actions of consumers. By utilizing confusing legal tools like terms of services that hide how companies use one's personal data, consumers are unable to fairly judge the privacy risks behind using an online service and are unable to easily control the data that is being collected. Additionally, the average consumer does not possess the same degree of technical knowledge regarding how consumer data is collected and used by companies and the U.S. government. As companies and governments can gather consumer data using a variety of different, sophisticated methods, consumers feel overwhelmed about being able to protect their privacy and have limited options

to take to fight back against the collection of consumer data, resulting in consumers giving up on protecting their privacy. Furthermore, consumers feel pressured to give up their data to use critical online services like search engines and to ensure that the government is able to stop national security threats, which normalizes invasive data collection in society.

Consumers' ability to change data collection regulations is affected by the limited spending power that consumers have compared to companies worth more than $1 trillion. As companies have donated large sums to political campaigns and formed relationships with politicians over countless years, it is almost impossible for consumers to convince lawmakers to enact meaningful data privacy regulations. These scenarios highlight the structural power imbalances that companies and the U.S. government hold over consumers to be able to change consumers' behavior, resulting in the privacy paradox.

The analysis of the privacy paradox shows how it should not be up to the consumer to protect their privacy. Instead, it should be the U.S. government's job to regulate consumer data collection because of the structural power imbalance among consumers, companies, and the U.S. government. As a democracy, the U.S. government should act according to the will of the individuals that the government represents, which includes protecting U.S. citizens from foreign threats. However, the U.S. government's actions in upholding national security by collecting consumer data at the expense of U.S. consumers' privacy ignores the feelings of a majority of consumers who care about their privacy and want their online data to be protected. The U.S. governments' inaction as a data collection regulator further illustrates how the U.S. government is failing to balance an individual's right to privacy with national security. Individually, American consumers lack the power to enact meaningful changes to how their data is collected. As the majority of American consumers are affected by the privacy paradox, a trigger event

similar in scale to the Snowden leaks will be needed to galvanize consumers to work together in consumer groups. By working with each other in concert, consumers can exert enough pressure to enact meaningful changes to privacy regulations before invasive data collection is inextricably linked to U.S. society.

References

Adkins, L. T. (2020, February 10). Federal government: More than the White House and Congress. *ShareAmerica*. https://share.america.gov/what-does-federal-government-do/

Alba, D. (2014, November 10). This device diagnoses hundreds of diseases using a single drop of blood. *Wired*. https://www.wired.com/2014/11/device-diagnoses-hundreds-diseases-using-single-drop-blood/

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. Telematics and Informatics, 41, 55–69. https://doi.org/10.1016/j.tele.2019.03.003

Bedrick, B., Lerner, B., & Whitehead, B. (1998, Spring). The Privacy Paradox. *The Reporters Committee for Freedom of the Press*. https://www.rcfp.org/wp-content/uploads/imported/PRIVPARADOX.pdf

Big Data. (2020, March 27). The Center for Insurance Policy and Research. https://content.naic.org/cipr_topics/topic_big_data.htm

Carpenter v. United States. (n.d.). *Oyez*. Retrieved April 6, 2021, from https://www.oyez.org/cases/2017/16-402

Cisco Annual Internet Report (2018–2023) White Paper. (2018). Cisco. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Clement, J. (2020, February 28). *Facebook: Advertising revenue worldwide 2009-2019* . Statista. https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/

Clement, J. (2020, February 5). *Google: Annual advertising revenue 2001-2019* . Statista. https://www.statista.com/statistics/266249/advertising-revenue-of-google/

Client Profile: Facebook Inc. (2020). OpenSecrets.Org; Center for Responsive Politics. https://www.opensecrets.org/federal-lobbying/clients/summary?cycle=2019&id=D000033563

Client Profile: Microsoft Corp. (2020). OpenSecrets.Org; Center for Responsive Politics. https://www.opensecrets.org/federal-lobbying/clients/summary?cycle=2019&id=D000000115

Greenwald, G. (2013, June 11). *Edward Snowden: The whistleblower behind the NSA surveillance revelations*. The Guardian. http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Greenwald, G., Ball, J., & Rushe, D. (2013, June 7). *NSA Prism program taps in to user data of Apple, Google and others*. The Guardian. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Griswold v. Connecticut. (n.d.). *Oyez*. Retrieved April 6, 2021, from https://www.oyez.org/cases/1964/496

International Statement: End-To-End Encryption and Public Safety. (2020, October 11). The United States Department of Justice; U.S. Department of Justice. https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

Jia, Y., & Weiss, R. (2019, May 15). *Introducing Translatotron: An End-to-End Speech-to-Speech Translation Model*. Google AI Blog. http://ai.googleblog.com/2019/05/introducing-translatotron-end-to-end.html

Lind, D. (2015, June 2). *Everyone's heard of the Patriot Act. Here's what it actually does.* Vox. https://www.vox.com/2015/6/2/8701499/patriot-act-explain

Litman-Navarro, K. (2019, June 12). Opinion |We Read 150 Privacy Policies. They Were an Incomprehensible Disaster. *The New York Times*. https://www.nytimes.chttps://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html

Lynskey, D. (2019, October 9). *"Alexa, are you invading my privacy?" – the dark side of our voice assistants*. The Guardian. http://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants

Madden, M., & Rainie, L. (2015, May 20). Americans' attitudes about privacy, security and surveillance. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Mitchell, A., & Diamond, L. (2018, February 2). *China's Surveillance State Should Scare Everyone*. The Atlantic. https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/

Myszczynska, M. A., Ojamies, P. N., Lacoste, A. M. B., Neil, D., Saffari, A., Mead, R., Hautbergue, G. M., Holbrook, J. D., & Ferraiuolo, L. (2020). Applications of machine learning to diagnosis and treatment of neurodegenerative diseases. *Nature Reviews Neurology*, *16*(8), 440–456. https://doi.org/10.1038/s41582-020-0377-8

Pagliery, J. (2017, October 19). *Tech companies are hindering criminal investigations, under outdated law*. CNNMoney. https://money.cnn.com/2017/10/19/technology/criminal-investigations-microsoft-ireland-invs/index.html

Paletz, D., Cook, T., & Owen, D. (2016). 9. 2 lobbying: The art of influence. In *American Government and Politics in the Information Age*. University of Minnesota Libraries . https://open.lib.umn.edu/americangovernment/chapter/9-2-lobbying-the-art-of-influence/

Privacy. (n.d.). Legal Information Institute. Retrieved April 6, 2021, from https://www.law.cornell.edu/wex/privacy

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, March 17). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Sweat, J. (2000, April 10). Privacy paradox: Customers want control—and coupons. *Information Week*.

Singer, N. (2018, April 11). What you don't know about how Facebook uses your data. *The New York Times*. https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html

Vinocur, N. (2020, June 29). *Why Trump's administration is going after the GDPR*. POLITICO. https://www.politico.com/news/2020/06/29/trump-administration-gdpr-345254

Weise, K., & McCabe, D. (2020, August 28). In bid for TikTok, Microsoft flexes its power in Washington. *The New York Times*. https://www.nytimes.com/2020/08/28/technology/microsoft-tiktok-lobbying.html

Wilf-Townsend, D. (2019, March 11). Perspective | The fine print that could undermine new Internet privacy legislation. *Washington Post*. https://www.washingtonpost.com/outlook/2019/03/11/fine-print-that-could-undermine-new-internet-privacy-legislation/

Williams, M., Nurse, J. R. C., & Creese, S. (2016). The perfect storm: The privacy paradox and the internet-of-things. *2016 11th International Conference on Availability, Reliability and Security (ARES)*, 644–652. https://doi.org/10.1109/ARES.2016.25

Wolford, B. (2018, November 7). *What is GDPR, the EU's new data protection law?* GDPR.EU. https://gdpr.eu/what-is-gdpr/