NAVIGATING DIGITAL MARKETING:
A COMPARATIVE STUDY OF US AND EU REGULATIONS

A THESIS

Presented to

The Faculty of the Department of Economics and Business

The Colorado College

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Arts

By

Tedy Reed

February 2023

NAVIGATING DIGITAL MARKETING:
A COMPARATIVE STUDY OF US AND EU REGULATIONS

Tedy Reed

February 2023

International Political Economy

Abstract

The United States and the European Union have different regulatory frameworks when it comes to digital marketing. More specifically, these two nations have varying attitudes towards certain types of consumer data collection, targeted marketing, Cookie preferences, and overall business ethics. This thesis looks at how business is affected by each nation's respective digital marketing protocols. Relying on eight interviews from experts in the digital marketing and privacy fields, this thesis will analyze the different experiences and opinions of these individuals in order to draw conclusions about the benefits and detriments of each nation's privacy regulations.

KEYWORDS: (Digital Marketing, Consumer Privacy, Data Collection Regulation, United States, European Union)

ON MY HONOR, I HAVE NEITHER GIVEN NOR RECEIVED
UNAUTHORIZED AID ON THIS THESIS

Signature

ACKNOWLEDGEMENTS

I would first like to thank my thesis advisor, Christina Rader for all of her wisdom, guidance, and support throughout this process. I would also like to thank both the Economics and Political Science departments at Colorado College for the time and effort they have put into my higher education. I am so appreciative of the time and aide that my participants provided; this study could not have been completed without them. Finally, I would like to thank my parents for all of the support, encouragement, and opportunities they have provided throughout my academic journey.

Table of Contents

Abstract ..... *ii*
ACKNOWLEDGEMENTS ..... *iv*
Table of Contents ..... *vi*
I INTRODUCTION *1*
II LITERATURE REVIEW *3*
US and EU Relationship *6*
Regulations and Public Policy *8*
Pros and Cons of Regulation in the Digital Era *10*
Research Design *13*
Population *13*
Interview Questions *15*
IV RESULTS *17*
Discrimination Versus Efficiency *17*
Choice *19*
Business *22*
EU vs US *26*
Ethics and Morals *28*
V DISCUSSION *33*
References *37*

CHAPTER I

INTRODUCTION

Back in 2012, Target gained significant publicity after consumers learned that the store utilized big data and predictive analytics in order to market better to their consumers, specifically their pregnant consumers. (Kuhn, 2023). Target was able to estimate pregnancies solely based off of a women's most recent purchasing patterns, and the store would then market specific products— such as cribs or diapers— to these consumers (Fernandez-Lamela, 2014). This was one of the first widely understood examples of targeted marketing. Through the last decade, businesses adopted Target's use of data and analytics in their own marketing strategies, specifically in digital marketing. Digital marketing refers to all marketing efforts that use electronic devices or the internet which allows businesses to provide consumers with personalized, relevant ads—as Target did. Digital marketing has proved to be quite beneficial for businesses and even consumers; however, the collection and manipulation of consumer data has raised global privacy concerns.

The best understanding about privacy across consumer, corporation, legal, and ethical domains is limited to US and European samples (Martin & Murphy, 2016). The privacy practices between the United States and Europe–specifically the European Union– are vastly different, yet research on global privacy and the effects it has on digital marketing are underdeveloped (Martin & Murphy, 2016). While digital marketing, in theory, is successful when consumer data is easily accessible, it raises the question of which facets and to what extent are businesses impacted when companies must work under the different regulations in the US versus the EU?

In order to better understand this topic, this thesis will gather information through interviews from individuals working within the global and domestic digital marketing industry. With the information provided from these interviews and literature gathered around privacy regulations based in the United States and European Union, a thematic analysis will be completed in order to better understand how varying privacy restrictions impact businesses and their marketing abilities. This study will face and analyze the qualitative research that is generated by the digital marketing field; thus, allowing for new questions and places to research to emerge.

This study anticipates to display the key differences between the US and the EU regulations and what led each state to those respective beliefs. Through these findings, the goal of this study is to be able to show how consumers and firms are affected/predicted to be affected by varying privacy legislation and how strategies surrounding digital marketing will prevail. The following chapter will provide a literature review including a thorough analysis of US and EU regulations, the benefits and detriments of regulations, and how consumers perceive privacy regulations. The third chapter will cover how data was collected and how it was interpreted. This chapter provides a list of the questions that were used in the interviews, along with background information on the professionals interviewed for this study. The fourth chapter will use thematic analysis to draw conclusions regarding the current state of digital marketing strategy when compensating for varying privacy legislations. Finally, chapter five will review the results and findings of the study, and suggestions about future research directions will be addressed.

CHAPTER II

LITERATURE REVIEW

Digital marketing, global privacy, and regulations have frequently been discussed in modern literature; therefore, it seems only appropriate to take these into consideration as well. This literature review will first address global standards for data privacy regulations–specifically in the European Union and the United States. Then, it will discuss how the differences in regulation affect the relationship between these two entities. The third section will examine public policy and how different countries choose to regulate. The final section determines the benefits and consequences of data regulation and how it affects digital marketing.

Standards

European Union

The European Union has set the gold standard for privacy law. As technology and data collection has developed at rapid speeds, the EU has been able to effectively adapt with the times. Upon the emergence of the Internet, the EU originally created the 1995 Data Protection Directive (The Directive) which at the time was considered the most powerful engine of global data protection (Birnhack, 2008). At its core, The Directive states that personal data must be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purpose; that the data collected is adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or further processed (Birnhack, 2008). In 2016, 28 EU member-countries passed the General Data Protection Regulation (GDPR) which officially replaced The Directive in May of 2018.

The GDPR is considered the most prominent example of a governing framework for collection, storing, and using personal data (Richards & Hartzog, 2019). The GDPR is founded upon six key principles: fairness and lawfulness; purpose of limitation; data minimization; accuracy; storage limitation; and integrity and confidentiality (Goddard, 2017). While The Directive provided a solid foundation for data security, the GDPR puts greater emphasis on transparency and accountability. Data can only be collected after consent is collected through a conscious and evidenced agreement. This now means more than clicking on an unticked box; it is now necessary to provide information regarding the details of the data recipients, retention periods, along with other information about personal privacy rights (Jerath & Choi, 2022; Goddard, 2017). In addition, this has to be disclosed in a clear manner with use of layman terms.

United States

In the United States, data privacy and protection—especially in the digital realm—is ambiguous and disorderly. Well defined federal regulations do not exist, making the United States the only democratic institution in the world to lack clear privacy laws. The nation currently relies on privacy regulations on an *ad hoc* basis rather than a proactive manner. US privacy guidelines are a mixture of Constitutional, state, contract, and tort laws (Hartzog & Richards, 2019).

Despite the lack of federal regulations, the United States is more so focused on public sector privacy and carries a laissez-faire attitude regarding the private sector. The US federal government follows a 'sectoral approach' where there are different regulations within the different economic sectors depending on what type of data should be protected (Fiero & Beier, 2022; Pop, 2022). For example, in the healthcare sector the Health Insurance Portability and

Accountability Act (HIPAA) protects patient privacy, or The Gramm-Leach-Bliley Act (GLBA) protects consumer data in financial institutions. The United States Constitution fails to explicitly mention the word "privacy" thus, privacy regulations are written within most state constitutions instead (Whiting, 2019).

California was the first state to initiate some form of privacy regulation that in ways mimicked the EU's GDPR. In 2018, California passed the California Consumer Privacy Act (CCPA) which became effective January 2020. The purpose behind the CCPA was to give consumers more control over the personal information that businesses collect and to secure new privacy rights for California consumers (CCPA, 2022). This regulation grants consumers the right to know (consumers are informed on the information businesses collect), the right to delete (consumers should be allowed to delete unwanted personal data that's been collected), the right to opt-out (consumers can request that businesses stop selling their personal information), and the right to non-discrimination (allows consumers to exercise their rights under the CCPA) (Jerath & Choi, 2022). Similar to the GDPR, businesses can face monetary penalties ranging from $2,500 to $7,500 for each violation against the CCPA (Jerath & Choi, 2022). In November 2020, voters approved the adoption of the CCPA with the California Privacy Rights Act (CPRA), which enforced a stronger and updated version of the CCPA. For example, the CCPA allowed for the right to opt-out, but the CPRA expanded the right to opt-out of all automated decision-making technology (Jerath & Choi, 2022). California alone has acted as a catalyst for comprehensive nationwide data privacy regulations, considering a myriad of business and tech giants are headquartered there. Since the approval of the CCPA and the CPRA, 18 other states have introduced similar bills (Hartzog & Richards, 2019), and similar legislation will become effective in Colorado and Virginia in 2023 (Fiero & Beier, 2022).

US and EU Relationship

In 2019, the US goods and services trade with the EU totals roughly 1.1 trillion USD (European Union, n.d.), making the United States and the European Union each other's largest trade and investment partners (Weiss & Archick, 2016). This is interesting considering the EU enforces firm data and privacy regulation through the GDPR, yet the United States' patchwork of privacy regulations is much less precise. While the EU views its privacy laws as non-negotiable, they recognize that an economically successful Transatlantic Trade and Investment Partnership (T-TIP) requires digital information to be shared between the EU and US.

In order to respect both data collection systems and the economic fruitfulness of T-TIP, there have been political agreements instituted over the last two decades that–in theory–allow for both. Originally upon the EU's passing of the Data Protection Directive in 1995, exportation of personal data was prohibited. This applied to all affiliates of US corporations, too (Hartzog and Richards, 2019). The United States was forced to change their business strategy within the EU which hindered business between both nations. The economic importance of US-EU relations became increasingly evident during this time period; thus, the Safe Harbor program was put in place in July 2000 to replace the Data Protection Directive. This agreement allowed "US companies and organizations to meet EU data protection requirements and permit the legal transfer of personal data between EU member countries and the United States," (Weiss & Archick, 2016). Without these agreements, the United States could not legally collect the data of EU consumers, let alone utilize the information for marketing purposes. Therefore, the Safe Harbor Program allowed the US to have more freedom while operating business in the European states, while still abiding to the privacy restrictions of the EU.

Throughout the past two decades, there have been numerous revisions to Transatlantic data flow agreements. In 2016, the Privacy Shield replaced Safe Harbor because the former was deemed invalid on the basis that it failed to meet EU data protection standards. The Privacy Shield included numerous revisions from the Safe Harbor program, but it overall emphasized stronger privacy protections and safeguards related to US government access to personal data (Weiss & Archick, 2016). As of 2021, US-EU negotiations continued regarding US-EU privacy framework because the US Government and the European Commission felt a need to intensify the regulations that are stated within the Privacy Shield, considering there continued to be privacy breaches from US companies (Privacy Shield Framework, n.d.)

It is evident that the US and EU have struggled to come to an agreement surrounding privacy regimes but refuse to give up on each other due to the significance of Transatlantic trade and investment ties. The US and EU hold completely different paradigms to be true, but their willingness to cooperate shows business is greater than these misalignments.

The EU has been the gold standard for data privacy regulation and has influenced significant data security legislation in Asia, the Caribbean, and Latin America (Greenleaf & Cottier, 2018). The EU has a grip on the rest of the world's privacy protection which can be argued is a byproduct of the "Brussels Effect"— a term coined by Anu Bradford that describes how European regulations play a direct role in imposing standards within the global market (Hartzog & Richards, 2019; Bradford, n.d). While the EU has taken global charge, the United States congress has remained reluctant to adopt any form of federal adaptation of the GDPR. While California and other individual states have implemented a *US analogue* of the GDPR (Jerath & Choi, 2022), the US and the EU exemplify that there are two cultures of privacy (Hartzog & Richards, 2019).

There is a key framework difference between the EU and the United States: the EU's priority is data protection, whereas the United States is more concerned with consumer and business protection. Europe treats privacy as a fundamental human right that should always be protected against governments and other private actors (Hartzog & Richards, 2019).On the other hand, there isn't a fundamental right to privacy in the United States as it is not included in The Constitution. Even if the United States strived to implement a federal version of the GDPR, there are implications included in data regulation that are in direct conflict with The Constitution. Article 17—right to erasure, also known as the right to be forgotten— of the GDPR is specifically viewed as a potential constitutional problem in the US because it can be seen as an infringement on the first amendment right to free speech because it threatens censorship (Hartzog & Richards, 2019). It states, "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay…" (GDPR, 2018).

Even with regard to the rudimentary differences between the United States and European Union, it doesn't mean the United States should avoid a comprehensive privacy legislative plan. In the midst of globalization, analysis and adjustments are almost always necessary when one country adopts public policy from another in order to best serve the needs of each country (Daniell, 2014).

Regulations and Public Policy

Public policy and national regulations are necessary keys to consider when understanding data and privacy collection. Despite their global interconnectedness, the United States—whose

regulation is more haphazard— and the European Union—the global model for privacy laws—display foundational differences regarding their respective privacy legislations. In order to understand the rationale behind each nation's preferences, it is crucial to recognize the purpose of public policy and the impact that national culture and history have on legal, political, and economic decisions.

There are various ways to perceive public policy. American author Harold Lasswell described it simply to be "who gets what, when, and how," (Daniell, 2014, p. 18). In other words, it seeks to understand specific choices governments and other political institutions make and to recognize both intended and unintended consequences of various policies (Daniell, 2014). There are deep historical roots within a society's legal and political culture; thus, it is inevitable that countries develop their own public policies based on culture (Daniell, 2014). Because there are so many distinct cultures and a country's culture and history play such a significant role in the ways it operates, public policy creates effective boundaries that are able to mediate through cultural differences (Daniell, 2014, p. 18).

In addition, public policy looks different throughout the world because neuroscience says that the brains of individuals from different cultures and locations operate differently, even when faced with the same problem (Andrews-Speed, 2022). It is understandable that the United States and European Union have taken varying action regarding public policy and data privacy; while both are developed, global giants, each state possesses a political culture and history that influences their respective public policies.

For instance, the European Union's past history with fascism and totalitarianism has influenced their views on data protection and "contributes to the demands of European politicians and publics for strict data privacy," (Weiss & Archick, 2016). The United States

views their history very differently; the United States is founded on the principle of personal freedom and non-interference by the state.

Pros and Cons of Regulation in the Digital Era

The question whether regulation is good or bad is relative, especially when the EU and US view it in very different ways. It has been noted that there is a Trans-Atlantic difference in rights, culture, commitments, and especially regulatory appetites (Hartzog & Richards, 2022).

Pros

In a digital era, many are skeptical when it comes to sharing their personal data; thus, we turn to regulation for protection. There is a variety of problems that are caused by data collection such as: vulnerability to fraud, privacy invasion, unwanted marketing communications, and obtrusive marketing communications that disrupt the rhythm of day-to-day activities (Martin & Murphy, 2016). In addition, in the United States where regulation is minimalized, consumers feel as if they have a lack of control over their own personal information which leads to distrust and dissatisfaction in businesses (Aridor et al., 2020; Martin & Murphy, 2016). Consumers report that there is actually a desire for greater government intervention related to privacy (Martin & Murphy, 2016). It is true that consumer data is what powers the digital economy, but it is also necessary that consumers have trust in a company's privacy protocols. Regardless of how strong a company's products are, a lack of consumer investment–both financially and providing personal information–will compromise the digital economy (Niebel, 2021).

Cons

On the other hand, while regulation may resonate better with consumers, there is clear evidence that supports personal data functions as an equivalent for monetary compensation (Hacker, 2019). When researching the effects of the GDPR, data was found that there was a 12.5% drop in click-through rates after the new regulations were instilled (Jerath & Choi, 2022), meaning there is less traffic on a company's website. While data regulation, along with regulation in general, is supposed to deter trusts and monopolies, it is actually harmful to small businesses. In order to comply with the guidelines outlined by the GDPR, there are complicated technical aspects that are often expensive, especially for small vendors. A study was completed that showed after one week of the GDPR implementation, "—websites' use of technology vendors fell by 15% because websites dropped smaller vendors. The higher compliance requirements led to a significant increase in the concentration of the vendor market, and this especially hurt smaller vendors." (Jerath & Choi, 2022). Small businesses are wary of violating GDPR protocols because violations come at detrimental costs, but for large businesses there are strictly positive economic values even when they commit violating acts (Hacker, 2019).

Privacy Paradox

Despite consumer outspokenness regarding privacy concerns, data shows that when given the option to opt out of data tracking, consumers rarely do. Even with regulation, consumers appear to be "not as reluctant" to tracking (Jerath & Choi, 2022). This behavioral phenomenon is known as the privacy paradox: the inconsistency between privacy attitudes and privacy behaviors (Kokolakis, 2017). In the United States, 91% of adults think they have lost control of their private information, and in the European Union, 57% of people have this same concern (Gerber

et al., 2018). With this said, globally "only 39% report to enforce high privacy settings on social networks, 34% turn off location tracking in apps, and only 18% try to avoid using popular data-gathering websites like Google and Facebook," (Gerber et al., 2018). By just looking at the results of the privacy paradox, it should encourage businesses to increase the collection and use of personal information, yet government policy makers justify greater privacy regulation on the people's raised privacy concerns," (Kokolakis, 2017). This ideology makes it difficult to justify whether consumers or businesses should have more say on how much regulation is really necessary or acceptable.

CHAPTER III

METHODOLOGY

Research Design

Because measuring the effectiveness of digital marketing, especially in different countries under different regulations is rather relative, this thesis focuses on qualitative research methods— specifically interviews— to gather proper and significant data from experts in the industry and hopefully, draw some form of conclusion. Qualitative research will provide us uncover underlying trends, reasons, and motivations. Interviews are interactive (Alshenqeeti, 2014) and allow the interviewer to ask for explanations and clarity while providing a place for discussions to be taken to any adjacent topics. This helped us grasp the clearest conclusion. While it may not provide hard evidence, this study is not limited to the numerical boundaries and allows for expert's information-rich opinions to be probed.

Population

This study gathered data from eight of individuals within the digital marketing, marketing, and privacy compliance industries. These respondents work for US companies that do business with both US and EU consumers. The eight experts varied across US geographical boundaries, industries, and specific job titles but are all well versed in the significance of digital marketing, and they all have dealt with the ambiguities of privacy regulation. Phone interviews, video interviews, and email interviews were completed to gather the necessary data. These interviews ranged between 30 and 60 minutes, depending on the available allotted time and how in depth the respondent answered the questions. The interviews were recorded–with consent

from the respondents– and transcribed in order to obtain as much accurate information as possible. Below, Table 3.1 provides a visual for each professional interviewed.

Table 3.1 Interview Candidates

Respondent	***Industry***	***Role***
JS	Redacted	Redacted
NL	Marketing and Public Relations	Founder and Owner
LB	Packaging and Healthcare	VP of Digital Marketing
AR	Commercial Lighting	Global Creative & Content Marketing Manager and Head of Marketing & Communication North America
AF	Digital Marketing and Paid Advertisement	Independent Marketing Consultant
MD	Technology	Product Lead for Privacy Centric Measurements
SL	Data Privacy Compliance	Privacy Consultant and Attorney
AD	Data Analysis	Redacted

Initially, there wasn't a specific sample size this study required. In quantitative studies, power calculations determine the necessary sample size for research, yet there aren't standards or requirements like this for qualitative studies (Malterud, et al., 2016). Rather, qualitative studies follow the idea of *information power*: the more information the sample holds, relevant for the actual study, the lower the number of participants needed (Malterud et al., 2016). While this is a convenience sample and does not represent the opinions of all businesses, the information gathered is still effective for this thesis.

Through networking with relevant contacts, eight eligible marketing experts from differing industries were chosen. These experts all came from different backgrounds and have faced unique experiences in their jobs but share the commonality of working through the assortment of digital marketing standards both domestically and internationally.

Interview Questions

The collected information is intended to show how privacy regulations impact the strategies and capabilities of digital marketing within corporations. These interviews were semi-structured; therefore, I provided a set of base questions, but adjusted them as needed during the interview. The questions were divided into four categories. The first section included basic questions regarding an introduction to the interviewee (ie: their role at the company) and the business they represent (ie: industry, size of the business). The second section referred to the role digital marketing plays and has previously played in the company's marketing strategies. The third section contained questions about consumers and their privacy concerns. These questions explored if businesses are aware of the worries consumers have regarding data collection and how they choose to respond. The fourth and final section is dedicated to discussing global and domestic privacy regulations. More specifically, the questions poke at how the different regulations between the US and EU affect not only how digital marketing is performed, but how it also affects the overall business. These questions all provided a framework to help spark conversation, but the discussions went further beyond these questions as experts were asked to take the conversation in any direction they saw valuable.

Table 3.2 Interview Questions

Questions Category	Interview Questions
Introduction and Background	● What is the size of the company? ● What industry are you in? ● What is your role at the business? ● Where is your firm based? ● How are you involved with digital marketing/privacy regulation at your firm?
Digital Marketing	● How has the shift towards digital marketing changed how your firm operates? ● Has there been a noticeable difference in the responses you receive from personalized advertisements?
Consumers and Privacy Concerns	● How does your firm approach consumer privacy concerns? From both a legal and ethical standpoint. ● What are your thoughts on the phenomenon coined the “Privacy Paradox”? In other words, when consumers are given the choice to opt-out of data tracking, only a small number of consumers actually choose to opt out. Their voiced privacy concerns do not match up with their actual actions. ● Regarding audience targeting, do you find this can ever become discriminatory or exclusionary in ways where only certain people get to see a promotion or a side of a company?

CHAPTER IV

RESULTS

Digital marketing has become a revolutionary strategy in the business world. While businesses have seen efficacious results from the data analytics that digital marketing offers, consumers are burdened by privacy concerns because of the significant amounts of data collected with every online interaction. There were five overarching themes that I derived from my interviews: discrimination vs efficiency, choice, the effect on business, the difference between the EU and US, and ethics. Throughout my results, I do report answers and insights from every professional interviewed, but there are some individuals who are quoted more frequently due to the thoroughness of their answers.

Discrimination Versus Efficiency

The concept of discrimination was a common discussion point through half of the interviews. In this case, discrimination refers to companies having the potential to provide consumers with different marketing offers but do it with ill intent. While all of the experts were posed the same question, the answers and opinions differed among the professionals. One out of the eight interviewed saw there to be big potential for malice use of consumer data. He saw that because digital marketing relies on targeting various audiences, it gives advertisers the ability to choose which consumers get to see what advertisements. JS stated some companies have so much information regarding their consumers that, “it becomes so powerful that you can then start to discriminate against certain populations, and you can start to build separate economies.”

On the other hand, out of the others that discussed discrimination, four of those interviewed believed that as long as companies operate under some form of “moral code,” ad

targeting is more so used for “relevancy versus discrimination,” (LB). NL provided an example of the benefits from ad targeting; one of her marketing clients is a school where the parent demographic is 90% Spanish-speaking. Thus, when marketing, her company makes sure there are Spanish subtitles on everything and that all ads are translatable. NL states “Yes, it’s targeting that specific demographic, but it’s in attempt to try to make it not feel exclusive to anyone.” Another expert argued that discrimination isn’t even relevant in this discussion. LB states:

> It's more around targeting the person that might get the most value out of what you're offering. It's less about trying to discriminate it against people [and] to attract the appropriate audience. It’s more about casting the right net to the people that will get the most value out of what you're offering from a product or a service standpoint.

The purpose of targeted marketing has always been efficiency—whether that be financially or having the flexibility to make quick changes to advertisements. LB continues:

> It's really not to exclude anyone, but for example, if we were doing a lot of hereditary cancer screening for women, I probably wouldn't target a man because he's not going to an OB office every year.

With digital marketing becoming a large phenomenon, it does raise concerns regarding how one’s data can be used against them without any knowledge or control over it, but as reported by eight different professionals who come from very different industries, targeted marketing is meant for efficiency rather than malintent.

Choice

What Choice do Consumers Have?

Choice—specifically for consumers— was a main discussion point for eight out of the eight professionals interviewed. In the United States specifically, there lacks conversation between consumers and businesses regarding privacy and the exchange of data. There is ultimately an unfair exchange between the consumer and the business because the business requires the consumer to grant access to their personal information in order to use the company's site.

For example, businesses utilize Cookies— **"**a small file or part of a file stored on a World Wide Web user's computer, created, and subsequently read by a website server, and containing personal information," (Webster Dictionary)—on their company websites in order to gain consumer information. Per JS, "It's really just a wall that comes up to incentivize the consumer to break down the wall as quickly as possible to get to the page they're wanting to reach." Additionally, LB stated, "[Consumer] data is being leveraged in a way that maybe they don't understand or don't like, but they don't know how to opt out." On websites, a pop-up will appear on the website and in order to access the main page, the consumer has to 'Accept All Cookies' (which in the US, is the default option) or the consumer can choose to 'Manage Preferences' which allows the consumer to pick and choose what information is tracked.

AF adds, "The intention with the Cookie prompt is to give the consumer the illusion of choice." Consumers do indeed have the choice to opt out of Cookie tracking, but unfortunately, in the United States, sometimes a website will require a consumer to 'Accept All Cookies' in order to access all of the website's features or even access the site at all. Thus, consumers do indeed have the choice to opt out of Cookie tracking, but at the expense of the good or service.

JS states, “If you aren’t going to get something that you need to work functionally on the site, you, the consumer, will allow [Cookies] because you want it to work the way the site should work.” LB seconds that US consumers look for convenience in everything which is why they are more likely to accept Cookies, but LB also states:

> It's just a lack of understanding to how things work from a technical standpoint… and the more you think about it, your own personal data is extremely valuable. I honestly think more people are against it, but then don't necessarily know what to do about it. And then in the EU, they're more advanced on helping the everyday person.

On the other hand, consumers under the GDPR are presented the Cookies upfront and have to consciously choose to be opted into data tracking. The functionality of the website is not affected if they reject the Cookies. Consumers in the EU are fully informed on their personal data collection and understand that they own their personal data; therefore, European consumers are able to make decisions regarding online data collection without feeling the need to exchange their private information.

It becomes more complicated in the US because it has never been made clear who owns the personal data: the consumer or the business that extracted it. If the US business owns the personal data collected, then a consumer truly does not have any choice when it comes to online tracking. AR argues, “The consumer doesn’t necessarily own the data, but they can and should at least own the initial decision on whether you want that person or company to track you.” Consumers and businesses are in a current limbo regarding data ownership, and while this remains the case, the US consumer has limited choices.

Even though the majority of conversations regarding digital marketing and data tracking are negative, when given the choice consumers often benefit from companies gathering their information; thus, consumers continue to be tracked. Digital marketing has continued to be revolutionary because "there are plenty of people who love being recommended cool, personalized items," (JS). Every professional interviewed claimed that there are multiple benefits for consumers that allow for their information to be utilized for targeted marketing. JS states that, "There are instances, where a consumer is given a choice not to have certain things tracked, but then they don't get the benefit." AF recognizes that there are many instances when people choose to be tracked:

> "Consumers know when they go to sites like *airbnb.com*- they want their geographic information tracked. On a trusted site they might always hit accept, but if they're doing a Google search and they come in through your website and they've never seen it before, they're probably going to be less apt to do it."

It is evident that all of the professionals agreed to some degree that consumers should be allowed to make their own decision regarding their targeted information when they want to accept the help or perks. From my interpretation, it appears that in digital marketing, choice should mean that when a consumer chooses to opt into a company's targeted marketing tracking, they will receive benefits and offers; however, when a consumer chooses to opt out, they should not be penalized in any way, such as not being able to functionally use the company's website.

Too Much Choice?

Per my interviews, it appears that in a perfect world, consumer choice would solve the relationship between businesses and consumers regarding privacy; however, my research shows that too much choice can be counterintuitive. For instance, JS disclosed, "A dirty trick of the Facebooks and Googles of the world is to give too much choice to consumers." He referenced one of Facebook's more recent Trust and Safety Initiatives which offered consumers an extensive list of options relating to what aspects of their data can be tracked. While choice is what majority of professionals believed was missing, JS notes, "By having more options, consumers choose to not make choices. I think Facebook did that because they understood that actually giving choice too much choice led to essentially consumer overwhelm where they don't make choice." SL adds that this is a similar phenomenon to a consumer's relationship with reading terms and conditions for any app or website. He notes, "Most people don't care about the terms and conditions. They 'read it' and they just say agree because they want to get to the product quicker." While companies technically provide the consumer with an outline of their data collection intentions, it appears these companies rely on the fact that consumers rarely read the terms and conditions before granting consent.

Business

Business has been impacted by both frameworks in the GDPR and the United States. Throughout my interviews, it appears that the GDPR does affect the sales, revenue, and overall consumer engagement for any company. In the United States, while business activity remains untouched, the inconsistencies in national regulation have created legal and greater monetary issues. Global companies feel the impacts of regulation discordance, especially when catering to both the US and EU. JS states, "Companies have to make these trade-offs: it's usually simpler to

do one size fits all across the whole world, but it's not great for business." As I heard from majority of those interviewed, it is incredibly expensive for any company to comply with every state or countries varying regulations; yet it also hinders business to abide by the strictest global privacy regulation (i.e., The EU).

Smaller Business Impact

Per four out of the eight I interviewed, the small and medium sized businesses take the greatest hit from inconsistent regulations. GDPR effects small businesses the most because it requires substantial legal and financial investments to comply with the specific regulations that are quite different from the US. AR revealed that many smaller companies that work with the EU believe target marketing in the EU isn't even worth it because it is "too much of an administrative hassle" and "is too costly compared the benefit." On the other hand, MD commented that her company's approach to global marketing solves for the lowest common denominator, or in other words, the strictest global privacy regulation. This is what most other large businesses do, but small and medium size business do not have the luxury to do such.

In the US, small businesses also face difficulties because most digital marketing requires the partnership with large online platforms such as Meta. In order to market on these platforms, companies have to front significant amounts of money which is feasible for large companies, but nearly impossible for smaller ones. LB describes ad platforms in the US—such as Facebook, Amazon, and Google—as "pay to play platforms" for businesses. LB continues by explaining that, "Your brand will not show up unless you give them money, and that hurt a lot of small businesses because it made it challenging to have a presence anywhere." In the US, these ad platforms are so valuable for businesses because they have first party data which allows them to

know for certain what consumers are not only buying, but also what consumers are browsing. LB reveals that her company budgets multimillions of their marketing funds to go to Facebook in order to stay relevant and gather useful consumer information. At the end of the day, the costs that businesses face in either the US or the EU are irrelevant if the company is large enough. SL summarized it as, "The big companies like Microsoft or Google have resources to it; it's everyone else that is affected."

The GDPR

Since the EU's adoption of the GDPR in 2018, global businesses have indeed noticed the impact it has had on their businesses. As AR describes it, "The GDPR was like a tsunami for anybody and everybody working in marketing." Four out of the eight individuals interviewed agreed that they have seen negative business effects when working under the GDPR. AR says that his company lost roughly 30% of their website users' data due to the GDPR Cookie policy. SL adds that the GDPR has hindered numerous clients and that while these regulations are meant to protects consumers, "—they add additional expenses and burdens to the company… It is a real problem for businesses."

Half of the experts stated that their respective companies do have a separate marketing strategy for the GDPR in order to combat or get around the strict regulations. For example, NL explains that companies put a greater emphasis on social media and celebrity sponsorships in order to market more freely to European consumers. She explains:

> "One way that you can get around [regulations] in places that have more restriction to focus your efforts more on social media or public relations in different ways by creating

> your own content. You don't necessarily have to hook onto Google or analytics quite as much there."

LB explains her company incentivizes consumers that visit their website to then sign-up for the company's newsletter. She describes, "What this allows you to do, is to be able to remarket to them through email." This method allows businesses to see the certain emails that consumers interact with the most and thus, consumer data is collected in a new way. LB describes: "This is how we could target hyper target. And that's how we were able to, in a very secure and compliant way." Overall, businesses that do continue to market in the EU are still able to find ways to interact with consumers despite the tight GDPR restrictions. AR believes, "Businesses are quickly adapting to the new scenario of not having as much data available."

In the United States, businesses continue to grow—especially when utilizing digital marketing—but companies are inhibited by the lack of national regulation cohesion. According to JS, "Businesses need certainty," which is almost nonexistent in the United States. States are able to change or create laws quickly, and if a company operates in various states (which almost all do), they must comply with all of the individual state regulations. Typically, companies choose to adhere to the most conservative state's laws which currently is California with the CCPA. JS further describes, "It's really hard when you operate a huge company when states have a lot of different ways to [regulate]." NL argues that "[Businesses] are rolling the risk that at any moment a state could pass something that we have to quickly get into compliance with or understand the risk of non-compliance."

Businesses of all sizes are affected by the incoherence of state regulation; however, NL expressed how she does sometimes appreciate the loose regulations in the US because it helps

drive revenue. She explains “We do focus the majority of our marketing efforts in the US because it's easier. There's less restrictions.” NL and LB both explain that companies generate the most revenue through target marketing which is significantly easier to do in the US in comparison to the EU. Therefore, businesses prefer the loose regulations in the US because it allows them to conduct strategies that will bring in the most money. NL said, “In the US, we're fairly loosey-goosey with [regulation]. We abide by our own set of ethics, and I guess I would call that better.”

EU vs US

Culture

Although US privacy is a growing area of interest among the general population, it is certainly not at the same level as Europe and probably will take some time to get to that place. 86% of the professionals interviewed utilized the word “pro-consumer” when describing the EU. In contrast, the US was described as trying to walk the line between the consumer and business, but with a lean toward business. While the US seems to have a pro-business approach, this doesn’t necessarily mean their regulations are anti-consumer. Per JS, “I do think that Americans culturally don't care about privacy. They care about getting stuff.” NL adds, “I think it's more of a function of our capitalist mindset here. Whatever is going to make businesses in the US successful, consumers are willing to deal with.”

Four out of the eight interviewees mentioned that the loose regulations are just a factor of US culture. The capitalistic drive that fuels the US is completely different from that of any country in the European Union. This is more of a US-global discrepancy rather than an inside US a political issue. One might assume that the US regulations in place are due to the political party in power; however, this is not a partisan issue. SL acknowledges that surprisingly neither

political party in the US has a vastly unique stance when it comes to data collection and privacy regulations. He states, "Colorado's what I would call a purple state. Utah is red and they have a [privacy] law. Virginia's volatile, they have a law. It's a concept in the US that has pretty bipartisan support. Most people think there will be a federal law at some point. It's just a matter of when."

US GDPR adoption

Throughout my research there were varying opinions surrounding a potential US adoption of something similar to the GDPR. Seven out of the eight experts believed a form of federal regulation would be beneficial. Some of the responses included:

NL: "Privacy is so much more established of a framework across the world and in certain states that it's silly not to have one at a federal level at this point."

AF: "[US regulations] need to be easier for companies to understand what they need to do to comply with the law and what it means and illustrate that."

AD: "It's the wild west of regulation and your interpretation of regulation and laws, and it's a moving target. Companies are trying to figure it out as best they can."

The United States plays an interesting role in digital marketing compliance: there is not a form of general regulation, however, companies often end up following the strictest guidelines. In reference to following both EU and US data regulations, AF states that, "It often has just been better to meet the strictest form of privacy across the board." This is also a similar experience for MD whose company also follows the most severe restrictions. This helps her company "maintain holistic reporting through conversion modeling."

Two interviewees made statements about how they expect the US to move towards a GDPR-esque framework. SL stated, “Companies just want simplicity. And that's why they're talking about the federal law. I think it will happen, but it's just a matter of time.” AD adds, “In the US, there are major pushes to kind of do what Europe is doing. But again, not fully under the terms of rights.” These two believe that the US is trying to balance the convenience of one set of guidelines with the ability to make business strides by utilizing digital marketing. Conversely, JS feels that the business culture in the US and EU is too different for anything like the GDPR to be adopted in the US. He argues that while digital marketing and the regulations surrounding it are being talked about, there isn’t any real or promising legislation that is being reviewed about it.

Others that I spoke with did agree with JS regarding how the conceptual differences between the EU and the US would make it difficult to implement anything like the GDPR in the United States. The biggest discrepancy between the two entities is the answer to who is the owner of data—is it the consumer or the platform that collected it? While discussing privacy differences between the EU and the US, AD described that data privacy is a right, thus, is included in the GDPR. This is fundamentally different in the United States where data privacy is just an extension of privacy rights – or the lack thereof. He states, “In Europe, they believe that data you generate belongs to you and is your ownership. But there’s nothing similar to that in the United States, yet.”

Ethics and Morals

Throughout all of my interviews, the most prominent theme to emerge was that of business ethics. This was a topic that 100% of the interviewed professionals mentioned. While the conversation centered around morals, there were two specific avenues that felt most salient: what is legal vs what is right and responsibility.

Legal vs Ethical:

When discussing digital marketing, the legal versus ethical debate surrounds the concept of what consumer data is accessible versus what consumer data is acceptable to use for target marketing. JS felt that this was the most important topic in the digital marketing conversation because companies are abiding by the law, but the consumer isn't necessarily protected. JS said:

> "There are companies that are, yes, following the laws, but it actually ends up being a really crappy experience for consumers. What companies are doing is technically legal and the laws are supposedly passed in the interest of a consumer, but it's not. When [regulations] come to life, it still feels like my privacy isn't being valued or protected."

LB shared that she was at the forefront of leading discussions with her company's compliance team when considering consumer privacy. LB says that the main focus was to decide what should they do vs what can they do based on the integrity the business chose to have. She gave the example that the compliance team decided it was fine to have ad platforms—such as Google or Facebook—put a pixel on the company's homepage to track consumer habits. It was not okay to share the consumer's personal data—such as health information—back to the ad platform. LB describes a time when her company chose consumer privacy and wellbeing over what was being asked of them. She disclosed, "I was actually in a situation where Facebook said to pass consumer health information back, and we told them no, we are not going to do that."

In my interviews, 100% of the interviewees mentioned the power that either Google or Facebook holds within digital marketing. I learned that these are the dominant ad platforms because "their information about consumers is so deep because they can watch behavior on their

own platforms to understand," (LB). To these large corporations, first party data—data that a company collects directly from its consumers—appears to be their main priority. Because the Facebooks and Googles of the world have access to considerable amounts of consumer data—arguably more data than necessary for targeted marking—it brings up questions concerning what data is okay to collect. JS believes, "giving consumers control over what data can or cannot be accessible is the missing piece to this all."

As I had learned earlier, there are companies who operate under two different marketing frameworks—one that complies with the GDPR and one for the United States. As we realized, this is because there are greater opportunities for business when targeted marketing is utilized, especially in the US. JS provided insight regarding the dissolute actions that he's seen occur on a global business scale. JS notes, "We always want to be able to have a consumer come in and still get all of the same choices they could across all of the geographies." This is in reference to companies who only consider consumer privacy when the law requires it. JS continues:

> For example, data deletion is only available for European consumers, but for us personally, that doesn't feel right. That is where I think we should take a European feature that we think is good and give it to US consumers too.

Responsibility

Throughout my eight interviews, different individuals brought to light who is responsible for making digital marketing more secure: the consumers, the businesses, or the government.

The majority of those interviewed would argue that the consumer holds the least responsibility when it comes to protecting or managing their own privacy, considering they don't have as much control or knowledge as the businesses or government. However, two

professionals did voice that in this digital world, there is a need for consumers to personally take accountability for protecting themselves. AF argues, “You have to take some level of personal responsibility and be careful with what you do on the internet.” She continued to explain that at least in the US, there isn’t an easy way to completely rid the internet of Cookies, so consumers need to be conscientious of what they are searching and what websites they choose to access. She notes that consumers do have the choice to decide which websites they can trust and which require more precautions. She states:

> “I think it's more of an indication of their relationship with that brand than it is about the privacy. Because if I went to National Geographic, I'd ‘Accept All’ … but if I'm on a [random website], I'm definitely going to manage my preferences.”

NL shared similar thoughts. She focused on the argument that if consumers have a smartphone or essentially any smart device, one’s privacy has already been compromised. She notes:

> I actually tell my clients that to anyone who has a smartphone, they already know everything about you, and they know what you want… You have to be off the grid if you don’t want people to know who you are.”

LB disagreed and voiced it should be the businesses who take ethics into consideration. She said, “It's definitely a company's responsibility to take ownership for making those ethical decisions.” The businesses are the ones with experts and technical understandings that consumers do not possess.

The third party that should hold responsibility is the government. However, over half those interviewed think the government should act as the last line of protection when dealing with digital marketing. Two experts argued that in a perfect world, businesses should be able to decide what is right and what is wrong to market on, but every business has their own version of what is moral. AF captures this when she said, “You can hope the website or the business will do the right thing but if not, you hope the regulations and the laws can protect the consumer in that respect.” Per SL, the government should also take a proactive approach in order to best protect consumers. He notes, “It’s a little bit up to the states and the leaders to educate people about privacy… the more people know about it, they will eventually exercise their privacy rights.”

CHAPTER V

DISCUSSION

This thesis examined the restrictions and regulations surrounding digital marketing and the impacts on business. It explored the relationship between the United States and the European Union in order to understand how consumers, businesses, and government are both affect and influence digital marketing on an international scale. The findings and conclusions drawn in this thesis come from the of data accumulated from the interviews of eight data and marketing professionals. There is a myriad of literature in academia regarding digital marketing, the GDPR, data privacy, and culture; however, there is a lack of literature that pieces all of these issues together through a business lens. With the help of the eight experts, this thesis was able to provide insight on how the different regulations in the US and EU impact businesses and provides behind the scenes insight on the motives and intentions of businesses when utilizing digital marketing.

In the past, there is an abundance of research revolving around the differences between US and EU privacy standards. The EU has proven itself to be the gold standard for data privacy and consumer rights (Hartzog & Richards, 2019) especially after the 2018 implementation of the GDPR. Meanwhile, the United States operates under a completely different strategy that leaves data and privacy regulations up to the states (Hartzog & Richards, 2019). There are fundamental cultural differences between the US and the EU, and this is why there is contrast between how the two nations operate in regard to digital marketing and consumer privacy. The EU views privacy to be intrinsic to every citizen, while there isn't anything of similar belief in the US. In addition, under the GDPR, a consumer's data belongs to them; therefore, consumers are allowed

to make decisions about who has access to their data and what they can do with it. The United States does not offer this same protection because there isn't any formal agreement that defines who does or does not own the consumer's data.

Both sets of regulations have their own influence on the success of a company. For instance, small businesses struggle with digital marketing in both the US and EU for different reasons. In the US, it is incredibly expensive for small businesses to afford to be advertised on large platforms. In the EU, it is incredibly expensive to hire lawyers or privacy consultants in order to ensure the company's marketing strategy is compliant with the GDPR. Therefore, smaller companies aren't as active in the digital scene; it is the corporations like Google and Facebook that can and do collect user data. Additionally, it is important to consider the ethics and motives of the companies utilizing user data. It became evident from the interviews that majority of companies have positive intentions in order to make the consumer experience better and more efficient through targeted marketing; however, there is always the risk that companies are collecting unnecessary personal data for greedy purposes.

Throughout the interviews, it became evident that digital marketing is still in its infantry stage; thus, the regulations surrounding it are also rudimentary. The EU has always carried a great pro-consumer ideology while the United States thrives on capitalism and big business. This is why the EU implemented a more developed privacy protocol such as the GDPR. The US appears to be in the midst of understanding what sort of regulations are most beneficial to promote business, protect consumers, and encourage a global economy. In the United States, there are different opinions on what is the right direction. Nevertheless, according to the eight interviews, it appears that more centralized and defined federal privacy laws are preferable and forthcoming.

As SL put it, “There is a divide between the EU and the US and not just by the ocean, but in terms of culture, specifically privacy culture.” This is proving itself to be true, but it doesn’t mean that the two nations can’t or should not work together. The digital era has forced the world to be so interconnected; therefore, businesses need to communicate between the EU and US. Despite their differences, the US and EU must reach an effective data agreement and build mutual trust in order to serve global consumers. While negotiations about Transatlantic data transfers are still occurring, it should be understood that the US-EU relationship is still incredibly strong, especially from a business perspective despite these fundamental differences.

Given all of the information, these interviews did provide a lot of answers, but there are most certainly still areas to further investigate. While my sample pool of eight experts provided relevant and incredibly insightful information, a larger sample size can always bring in additional opinions, especially if I had the ability to discuss these questions with a US government official or a consumer from the EU. Although, it should be noted that the participant demographics ranged greatly in age, industry, size of business, and location.

This thesis has provided a new piece of literature that has discussed the many avenues of digital marketing—such as culture, laws, and the main actors— and made connections to form an understanding on how they all can fit together. This study did provide some answers, but it also created a space for more questions to be formed. Some forward-looking topics that were inspired by the interviews include looking further into the tension between the economic cost of having to a universal data compliance protocol versus the costs of maintaining separate marketing strategies for different nations. If companies choose to comply with the strictest global regulations, they run the risk of losing consumers who do choose to opt out of data collection. On the contrary, if companies choose to have different marketing protocols for different

locations, they might be able to collect more data but will have to spend time and money ensuring they comply with all of the varying restrictions. In addition, if the United States does adopt a federal regulation—even if it is still more lenient than the GDPR—will this this instill more confidence within the EU to have more casual Transatlantic data transfers?

Digital marketing has revolutionized how companies communicate and interact with their consumers, and if used appropriately, will provide a more personalized and enjoyable experience for users. Hopefully, this study has provided a foundation for digital marketing research and will lead to a greater conversation surrounding user data privacy.

References

Alshenqeeti, H. (2014). Interviewing as a data collection method: A critical review. *English Linguistics Research*, *3*(1). https://doi.org/10.5430/elr.v3n1p39

Andrews-Speed, P. (2022). How may national culture shape public policy? the case of energy policy in China. *The Energy Journal*, *43*(3). https://doi.org/10.5547/01956574.43.3.pand

Archick, K., & Weiss, M. A. (2021, September 22). *U.S.-EU Privacy Shield and Transatlantic Data Flows*. Congressional Research Service. Retrieved November 3, 2022, from https://crsreports.congress.gov/product/pdf/R/R46917

Aridor, G., Che, Y.-K., Nelson, W., & Salz, T. (2020). The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3522845

Birnhack, M. D. (2008, September 24). *The EU Data Protection directive: An engine of a global regime*. Computer Law & Security Review. Retrieved November 16, 2022, from https://www.sciencedirect.com/science/article/pii/S0267364908001337

California Consumer Privacy Act (CCPA). State of California - Department of Justice - Office of the Attorney General. (2022, March 28). Retrieved November 16, 2022, from https://oag.ca.gov/privacy/ccpa

Choi, W. J., & Jerath, K. (2022). Privacy and consumer empowerment in online advertising. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4017940

Daniell, K. (2014, June). The Role of National Culture in Shaping Public Policy: A Review of the Literature. Australian National University.

Desai, D. M. V. (2019, April 18). *Digital Marketing: A Review*. International Journal of Trend in Scientific Research and Development. Retrieved November 16, 2022, from https://doi.org/10.31142/ijtsrd23100

Fernandez-Lamela, D. (2016, June 16). *Lessons from Target's pregnancy prediction PR FIASCO*. LinkedIn. Retrieved February 21, 2023, from https://www.linkedin.com/pulse/20140616204813-2554671-lessons-from-target-s-pregnancy-prediction-pr-fiasco/

GDPR. (2018, November 14). *Art. 17 GDPR - right to erasure ('right to be forgotten')*. GDPR. Retrieved November 16, 2022, from https://gdpr.eu/article-17-right-to-be-forgotten/

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Goddard, M. (2017). The EU general data protection regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, *59*(6), 703–705. https://doi.org/10.2501/ijmr-2017-050

Greenleaf, G., & Cottier, B. (2018, July 16). *Data Privacy Laws and bills: Growth in Africa, GDPR influence*. SSRN. Retrieved November 16, 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3212713

Hacker, P. (2019). Regulating the economic impact of data as counter-performance: From the illegality doctrine to the Unfair Contract Terms Directive. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3391772

Hartzog, W., & Richards, N. (2019). Privacy's Constitutional Moment and The Limits of Data Protection. *Boston College Law Review*, *61*(1687). https://doi.org/http://dx.doi.org/10.2139/ssrn.3441502

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the Privacy Paradox Phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Kuhn , G. (2023, January 8). *How target used data analytics to predict pregnancies*. Market Research Companies New York. Retrieved February 21, 2023, from https://www.driveresearch.com/market-research-company-blog/how-target-used-data-analytics-to-predict-pregnancies/

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies. *Qualitative Health Research*, *26*(13), 1753–1760. https://doi.org/10.1177/1049732315617444

Martin, K. D., & Murphy, P. E. (2016, September 22). *The role of data privacy in Marketing - Journal of the Academy of Marketing Science*. SpringerLink. Retrieved October 24, 2022, from https://link.springer.com/article/10.1007/s11747-016-0495-4

Niebel, C. (2021). The impact of the General Data Protection Regulation on Innovation and the Global Political Economy. *Computer Law & Security Review*, *40*, 105523. https://doi.org/10.1016/j.clsr.2020.105523

Office of the United States Trade Representative. (n.d.). *European Union*. United States Trade Representative. Retrieved November 16, 2022, from https://ustr.gov/countries-regions/europe-middle-east/europe/european-union

Pop, C. (2022, September 27). *EU vs US: What are the differences between their data privacy laws?* Endpoint Protector. Retrieved November 16, 2022, from https://www.endpointprotector.com/blog/eu-vs-us-what-are-the-differences-between-their-data-privacy-laws

Saura, J. R. (2020, August 15). *Using Data Sciences in Digital Marketing: Framework, methods, and performance metrics*. Journal of Innovation & Knowledge. Retrieved November 16, 2022, from https://www.sciencedirect.com/science/article/pii/S2444569X20300329

Weiss, M. A., & Archick, K. (2016, August 7). *U.S.-EU Data Privacy: From safe harbor to privacy shield*. UNT Digital Library. Retrieved November 3, 2022, from https://digital.library.unt.edu/ark:/67531/metadc855920/

Whiting, R. (2019). Don't Be Evil, Move Fast, Think Different: How Your Social Media Phone Applications Work Against Your Privacy. *Thomas Jefferson Law Review.*

Wright Fiero, A., & Beier, E. (2022). New Global Developments in Data Protection and Privacy Regulations: Comparative Analysis of European Union, United States, and Russian Legislation. *Stanford Journal of International Law,* 151–192.