Chapter 15
Managing Change Related to Consumer Privacy Laws: Targeting and Personal Data Use in a More Regulated Environment

Sophia Mueller, Charles R. Taylor, and Barbara Mueller

Abstract Internet usage among consumers, which encompasses a wide variety of activities ranging from social media to e-commerce, has exploded in recent years. Increasingly, marketers are using the trail of personal data consumers leave behind to achieve more precise marketing tactics and may even sell this information to third parties. This has led to growing concerns over the privacy of personal data. Despite a number of large corporations' data breaches—which should serve as a dire warning—many companies still do not take sufficient precautions when it comes to consumers' data. As consumer trust diminishes, some governments are taking a stand to protect data that until now, consumers have freely given away. In this environment, changes in the way data is collected and compiled are likely and will need to be managed. This chapter outlines a number of cases of data misuse, growing global concern over data privacy, and regulations that governments are already considering or have already passed to combat data mismanagement. Implications for marketers in this increasingly complex regulatory environment are outlined and recommendations given.

15.1 Introduction

On a daily basis, billions of people around the world use their computers and cellphones to access the Internet in order to conduct banking, make purchases, check the news or weather, and to keep in touch with family, friends, and colleagues.

S. Mueller (✉)
University of Florida, Gainesville, FL, USA
e-mail: smueller@ufl.edu

C. R. Taylor
Villanova School of Business, Villanova, PA, USA
e-mail: raymond.taylor@villanova.edu

B. Mueller
San Diego State University, San Diego, CA, USA
e-mail: muelle1@sdsu.edu

M. Karmasin et al. (eds.), *Media and Change Management*,
https://doi.org/10.1007/978-3-030-86680-8_15

In each case, the individual leaves behind personal data—the information trail that results from any type of Internet usage. Corporations use this information to achieve more precise marketing tactics—by targeting advertisements, offering rewards or discounts, and generally providing customers with a more personalized experience based on their individual preferences (see Terlutter & Ninaus in this volume). Some companies also sell this data to third-party data brokers. Such brokers gather information about a customer's behavior across multiple interactions with various entities: for example, a credit card company, car dealership, online shopping site, etc. This rich information about a consumer's behavior can be sold yet again. Moreover, the collection of consumer data has become ever more sophisticated, resulting in ever more detailed consumer profiles. Big data refers to enormous data sets that cannot be collected, stored, or processed using any of the existing conventional tools due to their quantity and complexity (see Green & Malthouse in this volume). The global big data market is forecasted to grow to $103 billion by 2027, more than double its market size in 2018 (Liu, 2019a). Big data analytics refers to the use of advanced analytical tools, such as predictive analytics and data mining, to extract value from big data and generate insights for firms. The benefits for firms are, of course, significant. According to the McKinsey Global Institute, it is estimated that data-driven organizations are 23 times more likely to acquire customers than their peers. These organizations are also six times more likely to retain customers and 19 times more likely to be profitable as a result (Bokman et al., 2014).

There is mounting evidence that companies capitalizing on data-based decision-making are on the increase. Indeed, according to a global survey, the adoption rate of big data has improved consistently every year from 2015 to 2018, with nearly 60c of organizations having claimed to use big data in 2018 (Dresner Advisory Services, 2018). A recent survey of US Fortune 1000 companies conducted by New Vantage suggests over 97% are investing in big data. And, success has led firms to up their investment in big data. New Vantage's survey indicated growth in the number of firms investing between $50 million and $500 million in such initiatives grew from 27% in 2018 to nearly 40% in 2019 (New Vantage Partners, 2019). According to the Worldwide Semiannual Big Data Analytics Spending Guide released by IDC, companies spent about $189 billion on big data and analytics (BDA) in 2019 (Liu, 2019b). This figure represents an increase of 12% over 2018, and estimates suggest worldwide BDA revenue will reach $274.3 billion (IDC, 2019). On a geographic basis, the USA is the largest country market by a wide margin with nearly $100 billion in BDA revenues forecast for 2019. Japan and the UK were expected to generate revenues of $9.6 and $9.2 billion, respectively, followed by China ($8.6 billion) and Germany (7.9 million). The fastest-growing big data and analytics markets are estimated to be Argentina and Vietnam (IDC, 2019). According to the same report, the industries accounting for the greatest share of big data and analytics revenues worldwide in 2019 were banking (13.9%), discrete manufacturing (11.3%), process manufacturing (8.2%), professional services (8.2%), and federal/central government (6.8%), with these five making up nearly half of the global revenue generation (Liu, 2019b). Between 2018 and 2022, the fastest growth is expected to come from investment services and retail. Retail's strong growth will enable it to move ahead of federal/central government as the fifth largest industry by 2022. In terms of company size, those corporations with upward of 1000 employees will be responsible for nearly two-thirds of all BDA revenues, while small- and medium-sized businesses will also be a significant contributor to BDA revenues, with almost a quarter of the worldwide revenue coming from firms with less than 500 employees (IDA, 2019). Firms unwilling to jump on the big data bandwagon face dire consequences. According to an Accenture study, 79% of executives agree that companies that do not embrace big data will lose their competitive position and could face extinction (Columbus, 2018).

Personal data is often compared to oil. Indeed, back in 2017, *The Economist* claimed that data replaced oil as the world's most valuable commodity (The Economist, 2017). When individuals use their computers and smartphones, they share endless amounts of personal data. Health records, social security numbers, and banking details make up the most sensitive information stored online. Less sensitive examples of personal data include social media posts, location data, and even search-engine queries. One aim of data collection conducted by firms is for the purpose of profiling customers and potentially targeting the promotion of goods and services to them based on their traits and habits. In some instances, the trade-off between the data that consumers share and the benefits they receive may be worthwhile: for example, when browsing online retailers, many consumers are happy to use "recommended for you" or "people who purchased this also bought" suggestions to aid in making purchase decisions. And, when consumers receive an ad regarding an airfare sale for a vacation destination they are interested in or a message calling attention to a newly released clothing item they find appealing, both the advertiser and the customer benefit. On the other hand, sometimes the use of big data misfires, as is the case when consumers scroll through their social media feed and find an apparel ad for a team that just beat their favorite team in a big game or when they receive notification of discounted hotel rooms after having already booked their reservation. But, when consumers realize their personal data has been shared with or sold to third (and in some cases, fourth) parties, it is no surprise that many become increasingly cynical about corporations' data protection claims, promises, and policies. Given the present environment, which includes increased concern about data collection, merging, and sharing processes, it is critical that companies consider how they will manage the situation.

15.1.1 The Misuse and Abuse of Personal Data

2018 was host to a number of high-profile data breaches that compromised billions of Internet user accounts. In each case, impacted firms suffered financial loses in the form of breach-related expenses, diminished stock value, and regulatory fines. Of much greater consequence was the loss of consumer trust. The Facebook-Cambridge Analytica scandal broke in March of 2018 when it was revealed that the London-based data-mining firm had harvested the personal data of up to 87 million Facebook user's profiles worldwide without their permission and used it for political advertising purposes. Cambridge Analytica obtained the information through an app that could identify the personalities of American voters and potentially influence their behavior. The data collected also included details on users' identities, friend networks, and "likes." The firm, hired by President Donald Trump's 2016 election campaign, used the data in an attempt to target audiences with digital ads and thereby influence election results. While Facebook routinely allows researchers to have access to user data for academic purposes (which users consent to when they create a Facebook account), the social media giant "prohibits this kind of data to be sold or transferred to any ad network, data broker or other advertising or monetization-related service" (Granville, 2018). Cambridge Analytica initially denied that they obtained or used the Facebook data, but later changed their story. Facebook demanded and received certification that the data had been destroyed and promised users it would make its pages and ads more transparent. It also made changes to its platform to restrict the information that app developers could access. Nonetheless, the Federal Trade Commission fined Facebook $5 billion—the largest fine ever imposed by the US consumer protection agency. The UK's Information Commissioner's office fined them another £500,000 (about $643,000), noting that UK citizen data was exposed to serious risk. Additionally, their stock price fell approximately 14% in the aftermath of the scandal, and both advertisers and users left the social media network.

In March of 2018, Google also faced a data scandal. Engineers within the company discovered a software bug in the Google+ social network, which exposed user information. The glitch gave outside developers the opportunity to access user's Google+ profile data for a whopping 3 years, between 2015 and 2018 (O'Flaherty, 2018). The bug was immediately repaired; however approximately 500,000 Google + private user's data (such as name, email address, birth dates, occupation, gender, age, relationship status, and profile photos) was made available to the public. Google initially chose not to disclose the leak to its consumer database or the public because it feared damage to its reputation as well as regulatory scrutiny. The scandal was ultimately revealed in a *Wall Street Journal* article in August, 6 months after the initial discovery. In November, Google revealed a second bug in the Google+ API that could have been abused to access the private data of over 50 million people. Google reported that the bug allowed apps, which were granted permission to view Google+ profile data, to incorrectly receive permission to view profile information the user had set to non-public. Once again the breach was quickly repaired and Google reported no evidence that the system was compromised by any third party. Due to the data breaches, Google+ was shut down by the social media network in 2019. In early 2019, Google was fined €50 million (around $57 million) by the French Data regulator CNIL (National Data Protection Commission) for violations of privacy laws. More recently in 2020, Google agreed to pay $7.5 million in a settlement to resolve a class-action suit brought against the firm (CISOMAG, 2020). It is no surprise that such scandals coincide with mounting privacy concerns around the globe.

15.1.2 Global Concerns About Online Privacy

Globally, concern over Internet privacy is generally high. In particular, Internet users globally are worried about risks to their online privacy: a recent survey found that 75% of Internet users from New Zealand, 70% from Canada, 68% from Australia, 66% from the USA, 65% from the UK, 62% from China, 61% from Germany, 61% from Mexico, 61% from Taiwan, 57% from the UAE, 56% from Japan, 55% from France, 52% from Italy, and 51% from Hong Kong were concerned (Clement, 2019a). Additionally, based on a survey of 25 economies around the world, it appears that such concern has only increased over the years. Comparing data from 2019 vs. 2018, 65% of Internet users in Latin America are more concerned about their online privacy as compared to a year earlier, while 63% of those in the Middle East and Africa had similar concerns. Nearly half (48%) of North Americans' concerns had increased, and a smaller percentage of consumers in Europe (39%) expressed growing concerns (Clement, 2019b).

While consumers realize they share vast amounts of digital data, they perceive various forms of data differently. A survey of adults in the USA, UK, Germany, and France found that 78% of consumers fear losing control over financial/banking data, 75% fear losing control over security information, and 70% fear the loss of identity information. Just over 60% (61%) fear losing control over medical information, and another 57% were concerned over the loss of their contact information. Boomers in the four markets surveyed cared more about these top five pieces of information than the other age groups. In contrast, Gen Zs expressed greater concern over information related to their location, as well as their photos and videos. An interesting aspect of this survey was that European attitudes toward data privacy were not uniform. The French were found to be less protective of their personal information than their German and UK counterparts across almost all categories of data surveyed (RSA, 2019).

Consumers are growing increasingly concerned about the benefits of sharing personal data, the security of their data, whether their data will intentionally or unintentionally be shared with third parties, comprehending company privacy policies, personal control over their data, and the laws in place to protect it (see Hattenberger & Vidreis in this volume). According to a recent survey by the Pew Research Center, a large share of US adults are not convinced they benefit from the widespread gathering of data (Auxier et al., 2019). Some 81% of American adults say the potential risks they face outweigh the benefits. And 79% of Americans report being concerned about the way their data is being used by firms. The majority of the US public is not confident that corporations are good stewards of the data they collect. For example, 79% say they are not very, or not at all, confident that companies will admit mistakes and take responsibility if they misuse or compromise personal information. There is also a collective sentiment that consumer data is less secure than in the past. Nearly three quarters (70%) of US adults say their personal data is less secure than it was just 5 years ago. And despite concerns, many Americans acknowledge they are not always diligent about paying attention to privacy policies. While nearly all Americans report being asked to approve privacy policies, only about one in five adults say they always (9%) or often (13%) read a company's privacy policy before agreeing to it. The survey also found a general lack of understanding about data privacy laws among the general population: two-thirds (63%) of Americans note they understand very little or nothing about the laws and regulations that are currently in place to protect their data privacy. With regard to the prevalence of tracking, 72% of Americans report feeling that all, almost all, or most of what they do online or while using their cellphones is being tracked by advertisers or technology firms of other companies. Finally, eight in ten Americans say they have very little or no control over the data companies collect about them. Consumers are reluctant to share information because they know little of how much of their information is collected, who gets to look at it, and what it is worth.

A corporation's privacy policies (or lack thereof) regarding the collection and use of data (including the sales to third parties) have significant impacts on consumers' behaviors regarding the sharing of data. A recent survey by Euromonitor of 40,000 respondents across 40 markets revealed that consumers are growing increasingly conscious about managing their personal data and restricting the type of information they share online. According to the survey, age plays a role in the degree to which consumers actively manage data sharing and privacy settings and the degree to which they freely share personal information online. Over 60% of those aged 30–44 reported actively managing data sharing and privacy settings. The youngest and oldest cohorts are less likely to actively manage the way their data is shared, suggesting they may be less concerned or less knowledgeable regarding how to monitor their privacy settings. Younger consumers tended to be more willing to share their data in exchange for personalized offers, but they expected transparency in how the data will be used. Those over the age of 60 were least willing to share personal information online (Byron, 2020).

Global concerns regarding the sharing of data are mirrored in the behavior of Americans. According to data collected by the US Census Bureau, up to 45% of households that engage in online activities reported that concerns about data privacy stopped them from conducting financial transactions, buying goods or services, posting on social networks, or expressing opinions on controversial or political issues via the Internet. Results of an Advertising Research Foundation (ARF) survey found that US consumers were less likely in 2019 to share personal information than they were just 1 year earlier, including even basic personal information. According to the ARF, the number of individuals willing to share their home address fell from 41% to 31% between 2018 and 2019. Those willing to share the name of their spouse decreased from 41% to 33%. Only 54% indicated they would be willing to share their email address—down from 61% the previous year (Swant, 2019).

A Euromonitor survey of consumers in 40 countries suggested that privacy concerns would be a top consumer trend for 2020 (Byron, 2020). But just who should be responsible for the security of consumers' data? According to a recent survey of consumers across ten markets and on four continents conducted by the Global Alliance of Data-Driven Marketing Associations and Acxiom, the answer to that question is, apparently, consumers themselves (Data and Marketing Association, 2019). When asked whether the government, industry, or individual consumers should have ultimate responsibility for data security, on average, 38% of consumers globally claimed they have ultimate responsibility for their own data security. Just 15% suggested that government institutions have ultimate responsibility, and a mere 5% believed that brands and organizations did. Just over one-third (35%) were of the opinion that such responsibility should be held by a combination of these options. However, views did vary across markets. Consumers in Spain and the Netherlands, for example, placed significantly more responsibility on government institutions. In comparison, consumers in Germany, Australia, the UK, and the USA were much more likely to suggest that consumers themselves should be the ultimate gatekeepers of their own data. Indeed, in the USA only 6% believed the ultimate responsibility should lie with government institutions, compared to 43% who claimed it should lie with consumers (Data and Marketing Association, 2019).

15.2 Regulation/Policy

In an environment where online privacy has garnered more scrutiny from global consumers in the past few years than ever before, especially in the context of marketing over the Internet, it is no surprise that the issue is receiving increasing attention from regulators. Europe has historically emphasized privacy as a basic human right, focusing on "opt-in" systems, whereby marketers were required to receive a consumer's consent to send them messages, whether by mail, phone, or via the Internet (Monahan, 1998). In contrast, the USA has traditionally emphasized a free flow of information, balancing the needs of marketers and consumers and requiring consumers to "opt-out" of receiving messages they do not want (Maynard & Taylor, 1996). Based on growing consumer concerns over data privacy, a number of governments are either considering, or have already passed, legislation aimed at restricting how marketers can collect and use consumer data. In particular, data management platforms (DMPs) have seen the brunt of regulatory attention, specifically pertaining to the degree to which they can be used to collect and merge data from consumers. However, due to the divergent beliefs of various governments, the degree of severity of these laws varies: it is unsurprising that the most comprehensive regulations pertaining to consumer privacy have been passed by the European Union. For some countries, these regulations are still in their infancy, while other nations and states, including California, have already passed legislation that is similar in spirit to that of the European Union's. Companies are being forced to adapt to these regulatory changes and face the prospect of additional regulation. In the following sections, these regulatory efforts are reviewed.

15.2.1 Europe's General Data Protection Regulation (GDPR)

After 4 years of debate, the General Data Protection Regulation (GDPR) was finally passed by the European Parliament in April 2016 and went into full effect as of May 2018. The regulation was significant in that it both codified and unified privacy laws across the European member nations. The overarching goal of the GDPR was twofold: (1) give EU citizens new rights to personal data, and (2) place restrictions on companies' use of consumer data for marketing purposes (Goldberg, Johnson & Shriver, 2019). Specific provisions of the GDPR included defining personal data, delineating consumers' data rights, placing limitations on data use by data controllers and data providers, requiring the use of "privacy by design" by data controllers, specifying breach notification procedures for enforcement, imposing penalties for breaches, and applying consumer rights to companies outside of Europe (Seaton, 2018; European Commission, 2020).

The GDPR defines personal data broadly as any information that is related to an identified or identifiable natural person. In this context, personal data can refer not only to basic identifiers such as an individual's name, email, address, phone number, or personal identification number, but is extended to include all information related to a person's identity, including mobile device identifiers or biometric data (e.g., fingerprints) (Seaton, 2018). The breadth of information that the definition encompasses is an important provision, as it addresses potential loopholes through which companies may have attempted to build data management platforms by merging individual level data that would otherwise not be covered under the regulation. Consumers are granted eight fundamental data rights under GDPR. Collectively, these provisions essentially force companies to obtain consumer consent to use or share their data, inform customers how their data will be used, and what their legal rights are if an abuse occurs (Johnson & Shriver, 2019). These rights are outlined in Chap. 3, articles 12 to 23 of the regulation, and include (European Commission, 2020; Urban et al., 2019):

- Right to Access Personal Data—refers to the ability to access data collected on them by a data controller.
- Right to Rectification—individuals can request modification of their data, including the correction of errors or updating of incomplete information.
- Right to Erasure—allows a subject to stop all processing of their data and request that it be erased.
- Right to Restrict Data Processing—allows requests to stop all processing of one's personal data.
- Right to be Notified—data subjects must be clearly informed about the uses of their personal data and informed of their rights.
- Right to Data Portability—allows individuals to request personal data be electronically sent to a third party.
- Right to Object—if a stop data processing request is rejected, an individual can object.

– Right to Reject Automated Individual Decision-Making—individuals can refuse the automated processing of their personal data by organizations to make decisions about them if it affects the data subject or produces legal effects.

Restrictions placed on companies' use of data under the GDPR are substantial. The "privacy by design" provision forces companies to explicitly build in compliance mechanisms into their data management procedures from their initial conception (European Commission, 2020). The breach notification provision forces a company to report to an agency within 72 h of a breach. Penalties for violations are significant, and fines can be as high as 4% of annual corporate revenue. The regulation also makes clear that it applies to countries outside the EU, encompassing both companies that are based in the EU doing business elsewhere and companies from outside the EU doing business within the EU.

15.2.2 The EU's ePrivacy Directive and Privacy Shields

Two additional aspects of regulation stem from the European Union—privacy shields and the EU's ePrivacy Directive. Prior to GDPR, the European Union had put forward the ePrivacy Directive (see ePrivacy Directive (2020) in 2002 (amended in 2009) which was designed to regulate data confidentiality, spam, use of cookies, information confidentiality, and related issues (Seaton, 2018). The main provisions of the Directive include providing security to users of online services, protecting the confidentiality of information, dealing with data retention by erasing or anonymizing traffic data when no longer needed, prohibiting the use of email addresses for marketing purposes unless the user has opted in, and regulating the use of cookies (Hintze, 2017). Historically, the ePrivacy Directive has been criticized for having enforcement issues. Recently, there have been efforts to update the ePrivacy Directive to be more clearly harmonized with GDPR.

A privacy shield is a framework that allows all companies from varying countries in a given transaction to transfer data through means that are compliant with all of the privacy laws that they must abide by. The most prominent example is the EU-US Privacy Shield Framework, which allows companies to opt in to join. The USA also has such an agreement with Switzerland. For US companies, this means self-certifying with the US Department of Commerce, which ensures that it is in compliance with Privacy Shield Principles. Privacy shields generally include a provision for penalties for noncompliance, which are enforced by the US Federal Trade Commission. The likelihood is high that other countries, or groups of countries, will develop privacy shields to help foster international trade.

15.2.3 The California Consumer Privacy Act (CCPA)

Following the lead of the European Union's GDPR, the California legislature passed a state law in 2018 that granted additional rights to consumers, including the ability to access or delete personal information collected by businesses and limit the sharing of such data. The law, which went into effect in 2020, grants consumers the right to know what data is being collected about them, the purpose for which it is to be used, as well as whether, and to whom, it is being sold (Pardau, 2018). It not only grants consumers access to their personal data but allows greater control over their data, including restricting who it will be sold to and the ability to delete it. An innovative provision included in the law is one that protects consumers from discrimination if they exercise their privacy rights (Williams & Irion, 2018).

In contrast to GDPR, to fall under the jurisdiction of the CCPA, companies must meet one of three criteria (State of California Justice Department, 2018). These criteria are fairly broad and consist of (1) gross revenues of more than $25 million, (2) engaging in the business of procuring or selling personally identifiable information on 50,000 or more people, or (3) earning more than half of their revenue from the sale of data. Companies covered under the Act must disclose what data they collect and obtain consent from consumers both to collect and share data. As with the GDPR, there is little doubt that the CCPA makes it considerably more difficult to collect data designed to create data management platforms that are used to target consumers in marketing communications based on merged individual data. Given that California is often a "laboratory for new ideas" (Williams & Irion, 2018), the implementation of the law will be closely watched, and some believe it will lead to additional protections in other states or even throughout the USA as a whole.

15.2.4 Vermont Data Broker Law (VDBL)

In 2018, the legislature of the state of Vermont passed a law specifically aimed at placing restrictions on data broker (Vermont Office of the Attorney General, 2018). Data brokers were defined as companies that knowingly collect personal information on consumers, which they subsequently sell or license to third parties (Vermont Office of the Attorney General, 2018). The legislation was designed to provide consumers with information about elusive brokers, so that they could opt out of having their information shared (Helveston, 2019). The law requires data brokers to register with the state, pay fees, and provide disclosures about their operations. The Law also strictly prohibits acquiring consumer information via fraudulent means. Violations of the VDBL can result in fines, and the Law grants those whose rights are violated the right to file civil lawsuits against data brokers (Helveston, 2019). While the VDBL is more narrowly targeted at data brokers, it is aimed at better protecting consumer privacy.

15.2.5 Other US States

In addition to California and Vermont, Nevada has recently passed a law (NevadaNRS § 603A.300) aimed at giving consumers more rights with respect to the use of their data. The Nevada law requires that those collecting data provide a request address to which a consumer can direct a request to opt out of the sale of individual data covered under the act. Lack of compliance can lead to civil penalties or injunctions. Additional states throughout the USA are beginning to pass data privacy laws, to varying degrees. According to the National Conference of State Legislatures, at least 20 states have passed legislation relevant to consumer privacy, including the areas of children's online privacy, e-readers, and websites (National Council of State Legislatures, 2020). Other states, including Georgia, are still considering legislation.

15.2.6 India's Data Privacy Framework and the Future

Inspired in part by the GDPR and the CCPA, other countries are seeking to strengthen their privacy protections. As of this writing, India is on the verge of passing a law related to data privacy, restricting how corporations can collect and share information on consumers. However, the legislation has been criticized by some. As the law exempts the government from its regulations, some believe that there is a move toward governmental control over the Internet (Goel, 2019). With the exception of the exclusion of the government from the regulation, the proposed provisions have some similarities with GDPR and CCPA.

It is clear that more attention is being paid to data privacy than ever before and the coming years will, no doubt, see other countries becoming involved in considering and/or passing such regulations. Below, we review how companies are managing change in data collection and consumer targeting in the current environment.

15.3 Reactions to the Trend Toward More Data Privacy Regulation

Considering the new privacy laws that have already gone into effect and those that will be doing so shortly, as well as potential data privacy laws that may be on the horizon, it is wise to consider the current attitudes of both consumers and marketing practitioners. As noted previously, many consumers are concerned about their online privacy (Boudet et al., 2019). Within the USA, consumers neither believe they have control over their data, nor do they believe that companies handle their private information responsibly, as the majority are convinced that firms are vulnerable to hacks and cyberattacks (PWC, 2017). This has led to a decrease in Internet usage among consumers (Boudet et al., 2019). Although they are willing to share their personal information when they trust a company, the majority of consumers in a national survey indicated that they would take their business elsewhere should that firm break their trust (PWC, 2017). Thus, marketers are facing consumers wary of their practices when it comes to personal data, though eager to provide such information should trust be at the core of the relationship. European consumers are fatigued with the onslaught of privacy notifications brought on by the GDPR, as more than 60% of popular websites display consent notices (Utz et al., 2019). This is a situation that consumers globally will need to contend with in the coming years. On the other side are the marketers who are required to put these new laws into practice. A recent survey of senior marketing leaders indicated that they may be viewing the data privacy world with rose-colored glasses: “64% said that they don’t think regulations will limit current practices, and 51% said that they don’t think consumers will limit access to their data” (Boudet et al., 2019). This may be an increasingly unwise stance to take, as the GDPR has already cracked down on British Airways and Marriott, fining the two companies $230 million and $123 million, respectively, representing roughly 1.5% of their global turnover (Fazzini, 2019). Additionally, Google was hit with a $57 million penalty in 2019 for a lack of transparency, and Facebook accrued a fine of $5 billion for their Cambridge Analytica scandal. These two tech giants are still under investigation by the EU for further infringements. Such fines are significant not only in terms of their monetary impact but also as a means for marketers to learn how regulators are interpreting broad laws such as the GDPR, which provided little guidance regarding implementation.

These data privacy laws, then, come with both benefits and drawbacks for marketers. There are indeed a number of challenges that marketers must consider. First and foremost is the cost of aligning internal policies with data protection legislation requirements. Particularly in the USA, a patchwork of individual state-level laws may create a legal environment that is increasingly difficult to navigate (Beckerman, 2019). And, all of these laws are subject to change, which will result in the ballooning cost of compliance over time. Furthermore, consumers may not be able to trust that their data is truly safe, as the mechanisms put in place to protect their data are by no means foolproof. Indeed, prior research has determined that identities can be stolen through the “Right of Access” clause in the CCPR (Pavur & Knerr, 2019). Currently, organizations do not have proper safeguards in place to deter abuse of this clause and “risk exposing sensitive information to unauthorized third parties” (Pavur & Knerr, 2019). The only way around this may be to ask for even more information from consumers, which counters the original intent of the laws (Hill, 2020). On the upside, a clear advantage for businesses are the positive effects the laws will have on consumers. Should a company properly implement data privacy protocol, consumers’ concerns surrounding the handling of their private information may be quelled, and trust in companies could increase, leading to an uptick in the data they allow marketers to collect. This will be particularly evident should the “privacy as a feature” strategy be put to use: “privacy functionality can be marketed as an additional product feature, emphasizing how the organization respects its users’ data by not selling information to third party suppliers” (Allison, 2019).

Additionally, through more rigorous requirements regarding data protection, companies will be less likely to fall prey to large-scale data breaches, which will result in both tangible (monetary) and intangible (reputational) benefits. Furthermore, the "significant resources saved by not being required to invest in costly data processing and associated administration" (Allison, 2019) are a major benefit to marketers. These savings can even extend to hardware costs, as companies will not require as much storage capacity. Although the drawbacks of data privacy laws are many, the overall benefits do outweigh these negatives. This has been documented through research, as "transparency and control in a firm's data management practices can indeed suppress the negative effects of consumer data vulnerability" (Martin et al., 2017, p. 36). Should a company fail to engage in data privacy measures, they will be left vulnerable to negative outcomes including abnormal stock returns. Additionally, consumers may undertake behaviors that are damaging to the company, including spreading of negative word of mouth, switching to another company, and falsifying information.

Moving forward with implementing these new data laws, marketers will need to adapt to three potential core areas of change: *data collection*, *data storage and processing*, and the *termination of a customer relationship* (Menon, 2019). First and foremost, the data collection process may look dramatically different for marketers in the near term. Consumers will need to be made aware of the data collection processes through informed consent, but marketers must be wary of overwhelming their customers by offering them too many different data privacy options (Utz et al., 2019). Prior research has indicated that the highest interaction rates with data privacy pop-ups come about when consumers are given only two options (though this will depend on a specific country's legal requirements). Such small implementation decisions will impact how consumers act with the content that a company provides. This process will place the customer in the driver's seat, as they will feel more in control over their data, reducing uncertainty and the perception of sneaky behaviors (Walker & Moran, 2019). However, due to the fatigue that customers are facing concerning the onslaught of data collection notices, we may not be far off from a comprehensive solution that provides more control relative to a yes/no answer, though does not impede the browsing of every single website a consumer visits (Utz et al., 2019). This will be particularly useful for transactions conducted on AI devices, where the number of parties involved in the purchasing process is increasing, and multiple consents will need to be in place (Sullivan, 2018). The type of data that is collected will also shift. Under the strictest data privacy guideline, the GDPR, "only data that is relevant, required, and limited to the conversion of a prospective buyer can be collected" (Menon, 2019, p. 80). Some marketers may wish to follow a different path and significantly reduce their dependence on data, while not falling to the "spray and pray" tactics of years gone by. One means of doing this is to alter the targeting format: marketers should consider centering their online advertisements on individual consumers as opposed to behavioral targeting.

Instead of leaning on traditional data management platforms, a marketer may wish to rely on the content of the web page or social media site that the customer is using. Content-based advertising capitalizes on the pairing of AI, content, and context-based data (Taylor, 2019a, 2019b). This works particularly well for video viewing websites, ranging from social media to streaming services. And, such marketing tactics may mean the annihilation of data platforms. Another novel technique is to incentivize consumers by paying them to watch advertisements via plugins (Taylor, 2019a, 2019b). This may allow the circumvention of advertising-blocking ad-ons, which were used by "more than 650 million people worldwide last year, costing advertisers an estimated $40 billion" (Taylor, 2019a, 2019b). Additionally, this reduces the likelihood of the archaic "spray and pray" from occurring, as consumers will be able to specifically avoid advertisements that they do not wish to see. Although new means of collecting data are quickly developing, it should be noted that laws surrounding data collection may become more stringent in the coming years, as they do not encompass all aspects of personal data. For example, the GDPR fails to include a number of ethical and privacy-related issues, including the collection of consumer data in order to determine their emotional state (Furey & Blue, 2018). Marketers must be aware of any and all changes to laws regulating data collection in order to maintain compliance.

Data storage and processing will also change rapidly, as marketers can no longer complacently store identifiable consumer data. Two options for storing data that some data privacy laws have put forward include anonymization and pseudonymization. Anonymized data includes sets of attributes of a consumer that cannot be linked directly to an individual. Pseudonymization "replaces identifying fields with a data record by one or more artificial identifiers" and is approved by such stringent regulations as the GDPR (European Data Protection Supervisor, 2018). Although these types of data storage options may lead to a fragmented data set, it can indeed still be processed to provide interesting consumer insights. Indeed, individual-level heterogeneity can still be culled from the raw data, resulting in new insights into consumer behavior (Kakatkar & Spann, 2019). However, marketers should proceed with caution when storing any type of data, either anonymized or pseudonymized. Particularly for anonymization, current methods of engaging in this scrambling of data may still be inadequate, as prior research has shown that with the plethora of data available to marketers, it may be significantly easier to pinpoint the correlation between data and consumer (Kolata, 2019). One recommendation to store and process data is to control access to the data set; another is to use secure multiparty computation.

Finally, marketers face a new challenge in customer relationships when specifically complying with the GDPR: complete termination of all data, should a consumer wish to pull their information. Although this may seem like a daunting task, particularly due to the fact that it costs more to acquire a new customer than to continue a current relationship, marketers should see this notion of terminating a customer relationship, or "forgetting" said customer, in a new light: as an "emancipatory process that will free pervasive computing from burdensome and pernicious disciplinary efforts" (Dodge & Kitchin, 2007; Politou et al., 2018, p. 12). Indeed, the inability to forget some information regarding a consumer's behavior may inadvertently hinder the customer relationship (Jeffries, 2011). This includes customers monitoring their behavior online, for fear of the data-driven repercussions.

Interestingly, current rules and regulations do not dictate a specific technique for terminating a customer relationship, allowing marketers a bit of wiggle room for the time being. Some recommendations for actively managing these customer relationships include using a privacy agent, attaching an expiration date to data, engaging in data degradation, or using block chain technology (Politou et al., 2018). A privacy agent acts as a software surrogate for the consumer, managing the data on their behalf. This allows consumers to actively manage their data from the start, making changing preferences and ending the relationship easier for both sides. Another way to forget consumer data is through expiration dates on information (Mayer-Schoenberger, 2009). This expiration date can be negotiated with consumers, who should be involved in all processes concerning their data. Another option is the idea of "data degradation," in which data can become desensitized through numerous degradation processes (Politou et al., 2018). This is based on the premise that marketers may still be able to engage in advertising initiatives even if the data is older, which is information that is generally less sensitive. This limited retention period and the degradation of information do have their drawbacks, however, as they cannot combat the age-old option of copying data and storing it elsewhere. Yet another option would be the use of the blockchain concept (Zyskind et al., 2015; Politou et al., 2018). This would allow customers to be in complete control of their personal data, with companies relieved of their duties to protect it or delete it once the relationship is over. This may be the ideal way for companies to engage with consumer data in the future, as the "decentralized platform makes legal and regulatory decisions about collecting, storing and sharing sensitive data much simpler because it is possible that laws and regulations are programmed into the blockchain itself, so that they are enforced automatically" (Politou et al., 2018, p. 18). Marketers have many options for terminating customer relationships, and it is presumed that many more will evolve in the coming years.

15.4 Conclusion and Future Outlook

For some three decades, academics have conducted research exploring the topic of data privacy. In an early attempt to increase marketers' understanding of privacy issues, Nowak and Phelps (1992) examined how well consumers are informed with respect to information gathering and practices. The extent to which the media covered consumer privacy issues was addressed by Phelps et al. (1994) in order to determine whether media salience of the issue led to public salience of the issue. At the turn of the century, an entire issue of the *Journal of Public Policy and Marketing* was devoted to privacy and ethical issues in database/interactive marketing and public policy (Milne, 2000). In that issue, Phelps et al. (2000) explored how consumers' willingness to provide marketers with personal data varied by information type. Milne (2000) focused on consumers' awareness of name removal mechanisms, such as opt-in and opt-out alternatives. Karson (2002) attempted to validate a scale of consumer privacy and security concerns on the Internet. A large number of investigations have focused on cross-cultural differences with regard to data privacy. Bellman et al. (2004), using a sample of Internet users from 38 countries, examined possible explanations for differences in Internet privacy concerns revealed by national regulation. Mahrous (2011) gathered data from Internet users in Egypt, the UK, and the USA.to determine how different levels of privacy concerns influenced actual purchase behavior. The influence of the content of online privacy statements on consumer trust was surveyed using Russian and Taiwanese subjects (Wu et al., 2012). Chen et al. (2013) focused on privacy issues among mobile phone users in the USA and Korea. And, Markos et al. (2017), using a cross-national survey of US and Brazilian consumers, developed a comparative study on information sensitivity and willingness to provide continua. An important contribution is that of Martin and Murphy (2017), who outlined the state or privacy scholarship in marketing and related disciplines, grouping theoretical perspectives and empirical findings about data and information privacy according to privacy's role in society, the psychology of privacy, and the economics of privacy. The authors suggest that our view of data privacy should not be constrained by consumer, organizational, ethical, or legal silos and propose expanding beyond these borders. In summary, consumer data and analytics are utilized and advanced by marketing practitioners at a rate that outpaces academic scholarship (Martin & Murphy, 2017).

As a result of the changes in the regulatory environment, it is more important than ever to study consumer privacy. Going forward, it will be important to focus on finding the right balance between effective targeting, which benefits businesses, and to some extent consumers as well, as they can get exposed to wanted as opposed to unwanted messages via better targeting. Both the potential benefits and the societal costs of privacy breaches should be factored into the equation.

This new frontier of data privacy, littered with a plethora of national and international regulations, is an area all marketers conducting business online will be confronted with. In the coming years, as the fallout from these regulations becomes known, researchers will have the opportunity to explore the laws themselves, consumers' reactions, as well as marketers' responses. In particular, research on consumer attitudes toward their data and specific privacy practices is needed. As policies become enacted, and consumers become ever more aware of their data privacy, marketers must develop a better understanding of consumers' attitudes toward both personal information and the laws that are there to protect it. Cross-cultural studies are needed to develop a richer understanding of country-based differences of data and data privacy. Additionally, there is a gap in the research regarding the effectiveness of corporations and industry trade associations taking on measures that attempt to balance consumer targeting with the protection of their data. The targeting vs. data protection debate is yet to be settled and can only be further complicated through its industry-dependent nature. Moving forward, it is particularly important for academic research to weigh in on the effectiveness of regulations in meeting their stated goals. The fallout effects of the current regulations are on the horizon and are an interesting area of future research. However, research conducted in the field of marketing will only become more challenging (Cuzzocrea, 2014). Although mining data from such social networking sites as Facebook and Instagram produces reliable insights, it will become more difficult to obtain as additional security measures may be put in place to align with upcoming regulatory requirements. When it comes to outsourced databases, problematic security issues may quickly arise, as "query processing procedures may easily access sensitive data sets and determine privacy breaches" (Cuzzocrea, 2014, p. 46). This is further complicated through the processing of any big data set, as analytics may quickly expose underlying consumer knowledge, so that the privacy of the consumer data is not preserved. Researchers will not have an easy time accessing information that will help them conduct studies on the data privacy frontier, as they themselves will have to deal with the implications of data privacy laws.

15.5 Exercise and Reflexive Questions

1. Develop a plan for effectively targeting European consumers with digital ads under the General Data Privacy Regulation from the perspective of a company outside the European Union.
2. Describe how you might better target consumers over the Internet via social media advertising while they are travelling on vacations under current privacy regulations.
3. Outline what you believe sensible privacy regulation would be for the USA as a whole given its history as an "opt-out" culture amidst growing concerns about privacy.
4. Since the writing of this chapter, which other countries (advanced or emerging) have passed laws to protect consumer data?
5. What are some additional repercussions of losing consumer trust due to data privacy issues?
6. What are the advantages of opt-in vs. opt-out systems of consumer consent?
7. Using the content-based advertising technique for your company or university, which pages would you target on web or social media sites?

References

Allison, P. R. (2019, July 9). *Data protection: How privacy can be a benefit, not a burden.* Computer Weekly. https://www.computerweekly.com/feature/Data-protection-How-Privacy-can-be-a-benefit-not-a-burden.

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. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Beckerman, M. (2019, October 14). *Americans will pay a price for state privacy laws*. The New York Times. https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html.

Bellman, S., Johnson, E., Kobrin, S., & Lohse, G. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society, 20*(5), 313–324. https://doi.org/10.1080/01972240490507956

Bokman, A., Fiedler, L., Perrey, J., & Pickersgill, A. (2014, July). *Five facts: How customer analytics boosts corporate performance.* McKinsey & Company. https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/five-facts-how-customer-analytics-boosts-corporate-performance.

Boudet, J., Huang, J., Rathje, K., & Sorel, M. (2019, November). *Customer-data privacy and personalization at scale: How leading retailers and consumer brands can strategize for both.* McKinsey & Company. https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/consumer-data-privacy-and-personalization-at-scale.

Byron, E. (2020, January 14). *Robots, mood enhancers and scooters: Top consumer trends for 2020*. The Wall Street Journal, A-11.

Chen, J., Zhang, R., & Lee, J. (2013). A cross-cultural empirical study of m-commerce privacy concerns. *Journal of Internet Commerce, 12*(4), 348–364. https://doi.org/10.1080/15332861.2013.865388

CISOMAG. (2020, January 10). *Google agrees to pay US$7.5M over Google+ data breaches.* CISOMAG. https://www.cisomag.com/google-agrees-to-pay-us-7-5m-over-google-data-breaches/.

Clement, J. (2019a, July 5). *Global concern about internet privacy risk vs. convenience 2018, By country*. Statista. https://www.statista.com/statistics/1023952/global-opinion-concern-internet-privacy-risk-convenience/.

Clement, J. (2019b, June 11). *Global opinion on concern about online privacy 2019, by region*. Statista. https://www.statista.com/statistics/373338/global-opinion-concern-online-privacy/.

Columbus, L. (2018, May 23). *10 charts that will change your perspective of big data's growth.* Forbes. http://www.forbes.com/sites/louiscolumbus/2018/05/23/10-charts-that-will-change-your-perspective-of-big-data's-growth/#1c4f3e892926.

Cuzzocrea, A. (2014). Privacy and security of big data: Current challenges and future research perspectives. *Conference on Information and Knowledge Management*. https://doi.org/10.1145/2663715.2669614

Data and Marketing Association. (2019, May 15). *Global data privacy: What the consumer really thinks*. DMA. https://dma.org.uk/research/global-data-privacy-what-the-consumer-really-thinks.

Dodge, M., & Kitchin, R. (2007). "Outlines of a world coming into existence": Pervasive computing and the ethics of forgetting. *Environment & Planning: Urban Analytics and City Science, 34*, 431–435. https://doi.org/10.1068/b32041t

Dresner Advisory Services. (2018, December 20). *Dresner advisory Services publishes 2018 big data analytics market study*. GlobalNewswire. https://www.globenewswire.com/news-release/2018/12/20/1670374/0/en/Dresner-Advisory-Services-Publishes-2018-Big-Data-Analytics-Market-Study.html.

European Commission. (2020). *Data protection in the EU*. European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.

European Data Protection Supervisor. (2018, March 19). *2017 annual report – Data protection and privacy in 2018: Going beyond the GDPR.* EDPS. https://edps.europa.eu/data-protection/our-work/publications/annual-reports/2017-annual-report-data-protection-and-privacy_en.

Fazzini, K. (2019, July 10). *Europe's huge privacy fines against Marriott and British Airways are a warning for Google and Facebook*. CNBC. https://www.cnbc.com/2019/07/10/gdpr-fines-vs-marriott-british-air-are-a-warning-for-google-facebook.html.

Furey, E., & Blue, J. (2018). Alexa, emotions, privacy and GDPR. In *Proceedings of the 32nd international BCS human computer interaction conference*. BCS Learning and Development Ltd..

Goel, V. (2019, December 10). *On data privacy, India charts its own path*. The New York Times. https://www.nytimes.com/2019/12/10/technology/on-data-privacy-india-charts-its-own-path.html.

Granville, K. (2018, March 19). *Facebook and Cambridge Analytica: What you need to know as fallout widens.* The New York Times. http://www.nytimes/2018/03/19/technology/facebook-analytica-explained.html.

Helveston, M. N. (2019). Reining in commercial exploitation of consumer data. *Penn State Law Review, 123*(3), 667–702.

Hill, K. (2020, January 15). *Want your personal data? Hand over more please.* The New York Times. https://www.nytimes.com/2020/01/15/technology/data-privacy-Law-access.html.

Hintze, M. (2017). In defense of the long privacy statement. *Maryland Law Review, 76*(4), 1044–1084.

IDC. (2019, April 4). *IDC forecasts revenues for big data and business analytics solutions will reach $189.1 billion this year with double-digit annual growth through 2022*. IDC. https://www.idc.com/getdoc.jsp?containerId=prUS44998419.

Jeffries, S. (2011, June 30). Why we must remember to delete – and forget – in the digital age. *The Guardian*. https://www.theguardian.com/technology/2011/jun/30/remember-delete-forget-digital-age.

Johnson, G., & Shriver, S. (2019). *Privacy & market concentration: Intended & unintended consequences of the GDPR*. *SSRN*. https://doi.org/10.2139/ssrn.3477686

Kakatkar, C., & Spann, M. (2019). Marketing analytics using anonymized and fragmented tracking data. *International Journal of Research. in Marketing, 36*(1), 117–136. https://doi.org/10.1016/j.ijresmar.2018.10.001

Karson, E. (2002). Exploring a valid and reliable scale of consumer privacy and security concerns on the internet and their implications for e-commerce. *Proceedings of the 2002 Academy of marketing sciences annual conference*, pp. 104–109. https://doi.org/10.1007/978-3-319-11882-6_36.

Kolata, G. (2019, July 23). *Your data was 'anonymized'? These scientists can still identify you*. The New York Times. https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html.

Liu, S. (2019a, August 9). Big data market revenue forecast worldwide 2011–2027. *Statista*. https://www.statista.com/statistics/254266/global-big-data-market-forecast/.

Liu, S. (2019b, July 22). Big data and business analytics market distribution worldwide 2019, by industry. *Statista*. https://www.statista.com/statistics/616225/worldwide-big-data-business-analytics-revenue/.

Mahrous, A. (2011). Antecedents of privacy concerns and their online actual purchase consequences: A cross-country comparison. *International Journal of Electronic Marketing and Retailing, 4*(4), 248–269. https://doi.org/10.1504/IJEMR.2011.045610

Markos, E., Milne, G., & Peltier, J. (2017). Information sensitivity and willingness to provide continua: A comparative study of the United States and Brazil. *Journal of Public Policy and Marketing, 36*(1), 79–96. https://doi.org/10.1509/jppm.15.159

Martin, K., & Murphy, P. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, 45*(2), 135–155. https://doi.org/10.1007/s11747-016-0495-4

Martin, K., Borah, A., & Palmatier, R. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Mayer-Schoenberger, V. (2009). *Delete: The virtue of forgetting in the digital age*. Princeton University Press.

Maynard, M. L., & Taylor, R. T. (1996). A comparative analysis of Japanese and U.S. attitudes toward direct marketing. *Journal of Direct Marketing, 10*(1), 34–44. https://doi.org/10.1002/(SICI)1522-7138(199624)10:1<34::AID-DIR3>3.0.CO;2-0

Menon, M. (2019). GDPR and data powered marketing: The beginning of a new paradigm. *Journal of Marketing Development and Competitiveness, 13*(2), 73–84. https://doi.org/10.33423/jmdc.v13i2.2010

Milne, G. (2000, March). Privacy and ethical issues in database/interactive marketing and public policy: A research framework and overview of the special issue. *Journal of Public Policy & Marketing, 19*(1), 1–6. https://doi.org/10.1509/jppm.19.1.1.16934

Monahan, P. A. (1998). Deconstructing information walls: The impact of the European data directive on U.S. businesses. *Law and Policy in International Business, 29*(1), 275–277.

National Council of State Legislatures. (2020). State laws related to internet privacy.. *National Council of State Legislatures*. https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

New Vantage Partners. (2019). *Big data and AI executive survey 2019.*. New Vantage Partners. https://newvantage.com/wp-content/uploads/2018/12/Big-Data-Executive-Survey-2019-Findings-Updated-010219-1.pdf

Nowak, G., & Phelps, J. (1992). Understanding privacy concerns: An assessment of consumers' information-related knowledge and beliefs. *Journal of Direct Marketing, 6*(4), 28–39. https://doi.org/10.1002/dir.4000060407

O'Flaherty, K. (2018, October 9). Google+ security bug – What happened, who was impacted and how to delete your account. *Forbes*. https://www.forbes.com/sites/kateoflahertyuk/2018/10/09/google-plus-breach-what-happened-who-was-impacted-and-how-to-delete-your-account/#6188e8ab6491

Pardau, S. L. (2018). The California consumer privacy act: Towards a European style privacy regime in the United States? *Journal of Technology Law and Policy, 3*(1), 68–114.

Pavur, J., & Knerr, C. (2019, December 2). GDPArrrrr: Using laws to steal identities. *Blackhat USA whitepaper*. arXiv:1912.00731.

Phelps, J., Gonzenbach, W., & Johnson, E. (1994). Press coverage and public perception of direct marketing and consumer privacy. *Journal of Direct Marketing, 8*(2), 9–22. https://doi.org/10.1002/dir.4000080204

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy and Marketing, 19*(1), 27–41. https://doi.org/10.1509/jppm.19.1.27.16941

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, 1–21. https://doi.org/10.1093/cybsec/tyy001_1

PWC (2017). *Consumer intelligence series: Protect.me*. PWC. https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf.

RSA. (2019). *RSA data privacy & security survey 2019: The growing disconnect between consumers and businesses.* RSA. Rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf

Seaton, E. E. (2018). Mind your businesses: Why Georgia companies should worry about European privacy law. *Georgia Journal of International and Comparative Law, 47*(1), 247–264.

State of California Justice Department (2018). California consumer privacy act (CCPA). *Office of the Attorney General*. https://oag.ca.gov/privacy/ccpa.

Sullivan, C. (2018). *GDPR regulation of the use of AI and deep learning for IoT data processing – A risky strategy. Project #TR-329*. S'ERC Technical Report.

Swant, M. (2019, August 15). *People are becoming more reluctant to share personal data, survey reveals.* Forbes. https://www.forbes.com/sites/martyswant/2019/08/15/people-are-becoming-more-reluctant-to-share-personal-data-survey-reveals/#4055bd431ed1.

Taylor, C. R. (2019a, July 29). *Can artificial intelligence eliminate consumer privacy concerns for digital advertisers?* Forbes. https://www.forbes.com/sites/charlesrtaylor/2019/07/29/can-artificial-intelligence-eliminate-consumer-privacy-concerns-for-digital-advertisers/#40967401b264.

Taylor, C. R. (2019b, April 1). *Will advertisers of the future need to pay consumers to see ads?* Forbes. https://www.forbes.com/sites/charlesrtaylor/2019/04/01/will-advertisers-of-the-future-need-to-pay-consumers-to-see-ads/#1dc741c72d72.

The Economist (2017, May 6). The world's most valuable resource is no longer oil, but data. *The economist*. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

Urban, T., Tatang, D., Degeling, M., Holz, T., & Pohlmann, N. (2019). A study on subject data access in online advertising after the GDPR data privacy management. *Cryptocurrencies and Blockchain Technology*, 61–79. https://doi.org/10.1007/978-3-030-31500-9_5

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed consent: Studying GDPR consent notices in the field. In *ACM conference on computer communications security* (pp. 973–990). ACM.

Vermont Office of the Attorney General. (2018, December 11). Guidance on Vermont's Act 171 of 2018 data broker regulation. *Vermont office of the attorney general*. https://ago.vermont.gov/wp-content/uploads/2018/12/2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf

Walker, K., & Moran, N. (2019). Consumer information for data-driven decision making: Teaching socially responsible use of data. *Journal of Marketing Education, 41*(2), 109–126. https://doi.org/10.1177/0273475318813176

Williams, J., & Irion, K. (2018). *Dream of californication: Welcome to the California consumer privacy act. Policy review*. https://policyreview.info/articles/news/dream-californication-welcome-californian-consumer-privacy-act/1351.

Wu, K., Huang, S. Y., Yen, D., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior, 28*(3), 889–897. https://doi.org/10.1016/j.chb.2011.12.008

Zyskind, G., Nathan, O., & Pentland, A. (2015). *Decentralizing privacy: Using blockchain to protect personal data* (pp. 180–184). IEEE, Security and Privacy Workshops.

Sophia Mueller is a Ph.D. student in the Department of Advertising in the College of Journalism and Communication at the University of Florida. She previously completed her Master of Business Administration at San Diego State University. Her research on cross-cultural differences in international advertising and marketing practices has been presented at conferences globally.

Charles R. Taylor is the John A. Murphy Professor of Marketing at the Villanova University of Business and Senior Research Fellow at the Center for Marketing and Consumer Insights. He currently serves as Editor in Chief of the *International Journal of Advertising*. Professor Taylor is a Past-President of the President of the American Academy of Advertising. He is the recipient of the Ivan L. Preston Award for Outstanding Lifetime Contribution to Advertising Research from the American Academy of Advertising and the Flemming Hansen Award for Outstanding Contribution to Advertising from the European Advertising Academy. Professor Taylor is frequently quoted in the media and contributes a column to Forbes.com.

Barbara Mueller is a Professor of Advertising at San Diego State University. She has published more than 60 book chapters and journal articles. Her scholarship has appeared in *the International Journal of Advertising, the Journal of Advertising, the Journal of Advertising Research, the Journal of International Marketing,* and *the Journal of Promotion Management*, and she serves on two editorial review boards. Additionally, she is the author of *Dynamics of International Advertising: Theoretical and Practical Perspectives* (Peter Lang, 3rd Edition, 2017, as well as two additional textbooks. She has taught courses in international advertising and international consumer behavior in Austria, Malta, and Finland and lectured in Germany and the Ukraine.