GDPR and Data Powered Marketing: The Beginning of a New Paradigm

Mohan Menon
University of North Georgia

Data has become lifeblood of marketing. In the recent past, there has been a proliferation of data and privacy breaches at companies of varying sizes. From the massive breach at Equifax to the day-to-day hacks, consumers are faced with an uncertain fate of their personal information. While there is a lack of action in the U.S., European Union is trying to tackle the issue with the General Data Protection Regulation (GDPR). It is likely to cause marketers to rethink their data policies. The manuscript addresses the elements of GDPR and some of the implications for marketers.

INTRODUCTION

Consumers in Europe and to some extent in the US have been seeing "change of terms" emails and pop-up consent links from companies about updates to privacy policies that hitherto were ignored by them. A recent survey of consumers by Deloitte found that 91 percent of them click their consent to Terms of Service (ToS) and Privacy Policy (PP) conditions without reading them (Business Insider 2017). Among the 18-34 year-olds the number was 97 percent. In another study, Obar and Eldora-Hirsch (2016) concluded that the reading times for the average ToS and PP were in mere seconds and consumers are eager to click through to the site/app. While companies use legalese to protect themselves, consumers click them because they might not have a choice if they want access to the site or use the apps' services. But are they giving away the farm! Recent revelations regarding Facebook data poaching and its ultimate use in manipulating voter sentiments seem to have brought the issue to the fore. In 2013, researcher Aleksandr Kogan accessed user data, shared it with Cambridge Analytica, and a scandal was born.

Post-revelations, Facebook suspended 200 apps for possible data misuse (Hubspot 2018). According to the article, the actions were the result of a full investigation of apps that accessed "significant amounts of personal user information prior to their 2014 policy changes" (Hubspot 2018). But that might not be the whole story. During the Congressional testimony regarding the Cambridge Analytica breach, the company maintained that users' information had been "walled-off" on May 15, 2015 and issued a public apology. Yet, recent revelations indicate that Facebook was sharing user data, beyond May 2015, with sixty or so device makers, including Chinese phone maker Huawei, which had been banned in the U.S. In another instance, Wall Street Journal (2018) reported that Facebook had separate "whitelisted" customized data sharing agreements (including friends' data) after the May 2015 with companies such as Royal Bank of Canada, Nissan Motor Co. who advertised on the site. The question points to the credibility of companies' public statements and mea culpas.

Things might be changing at least in the European Union. Marketers are being forced to reflect on their privacy policies following the establishment of the EU's General Data Protection Regulations

(GDPR). With a steady slew of hacking and data breach incidents, consumers are right to worry about personal information being held by companies and others that might have access to them. From unwanted emails or spam to big data breaches (ex. Equifax), marketers on- and off-line will be affected. Marketers need to explain to consumers why they are collecting personal data, how it is going to be used and with whom the data will be shared. Websites, apps, and other properties that allow consumers to interact with company media/stores will be affected. For instance, the current "dark patterns" that passively compel consent, like pre-checked boxes, are explicitly banned" (New York Magazine 2018).

Consumer Privacy or Lack Thereof

The Economist calls consumer data the most important resource in the world and advocates a new approach in the era of 'data economy' (2017). As computers, smartphones, automobiles, other connected devices and appliances (IoT) connect to the 'Net, there are quintillion bytes of information passed on to the servers each day. As the 'Netizen population grows to over 3.5 billion humans, there is more data being generated every second, minute, and day. The estimates are that ninety percent of data in the world in 2017 was created just in the previous two years and that the US alone generated over 2.6 billion gigabytes of Internet data every minute (Hale 2017). A self-driving car will alone generate 100 gigabytes of data per second (The Economist 2017). Given the volume of data being generated from each device, marketers will increasingly be dependent of Machine Learning (ML) and artificial intelligence (AI) to make sense of it all and potentially monetize it through consumer and machine behavior prediction.

To the extent that data can be collected about products, their usage, and the behaviors of consumers, a company can create competitive advantage in the market. For instance, Tesla, despite selling a fraction of the cars compared to GM or Ford, has a market valuation in the same territory (Seeking Alpha 2018). The difference is the driver and machine data that Tesla can acquire in order to make better cars and provide customers better driving experience. A McKinsey whitepaper on monetizing data from cars predicts that, by 2030, the overall revenue from car data would be $450b - 750b globally (2016). These networked cars, devices, and appliances of 2018 may be seen as rudimentary as industry marches toward enhanced data-driven approaches that make the machines safer albeit less private.

The need for monetizing data has to be balanced with the need for data protections. If not, both the consumer and the company are likely to lose in the long run. The unfathomable quantity of data collected today is ripe for abuse both by well-meaning actors and those with questionable and downright criminal motives. About forty seven percent of all data breaches in 2017 were caused by malicious or criminal attacks" (Jacob 2017). According to an industry study, the average cost of data breach in 2017 was $3.62 million and the cost for each lost or stolen record containing sensitive and confidential information was $141 (Jacob 2017). According to this study, European nations experienced the most significant decrease in average costs.

While it is easier said than done, data protection and security are daunting tasks given the nature of the underlying infrastructure. Data mirroring and distributed computing that creates redundancy and quicker access, might also pose a security risk. For instance, Amazon maintains a geographically dispersed data center operation spread across 12 regions with multiple data centers within each. Given the distributed nature of data storage, businesses find it difficult to delete customer data and many of them don't have systems in place to do so (MacDonald 2018).

At the same time, governments' need for economic and physical security leads to more data being collected about each individual. While no security system is one-hundred percent fool proof, data intrusion incidents by employees and outsiders at the National Security Agency (NSA) demonstrate the need for higher levels of security protocols to protect individual data (Shane, Perlroth and Sanger 2017). While, there are very legitimate reasons for data collection/storing/processing, nevertheless the lack of anonymity, theft & sale of information, cost of getting life back to normal, etc. are often overlooked.

Business' Responses to Data Breaches

Studies on consumer sentiments after data breaches have shown that older consumers tend to be more aware of a breach than younger ones and that both men & women had greater awareness of breaches

involving merchants/stores they frequented (Santarcangelo 2016). Surveys have shown that, in general, consumers feel companies are to blame since they do not take data security seriously, that they are willing to shop elsewhere and some consider taking legal action (Hart 2018). In the wake of the Cambridge Analytical debacle, sixty nine percent of consumers polled wanted to see European style data privacy laws enacted in the U.S. (Janrain 2018). Similarly, in a Harris poll, eighty three percent of Americans wanted tighter regulations and penalties for privacy data breaches and eighty four percent wanted companies to be held liable for the content within their servers (Breland 2018). Finally, according to a CBS News/YouGov survey, sixty percent said that Facebook's response to data breach is unacceptable and that the company should do more to protect data (De Pinto 2018).

Sometimes, consumer might take matters in their own hands. In the wake of the Russian ad buying and Cambridge Analytical revelations, #deletefacebook was trending, app and Website sign-on using Facebook credentials dropped. Sites/apps such as Socialive, UniDosh, and Bumble Trading have all reported lower numbers of Facebook enabled sign-ins. (Bloomberg Businessweek 2018). Social media sign-on functionalities, while convenient, also allows third-party developers to access user data. This breeds a co-dependency between Facebook and its platform-centered apps.

Responses from businesses regarding data beach or privacy violations have been deficient. U.S. consumers might have seen recent TV ads from Well Fargo, Facebook, and Uber expressing regret with over data breaches and other wrongdoings. These 'mea culpa' ads can be seen on multiple channels/platforms and cost millions of dollars. Public relations experts say that the first step in apologizing for a situation is to admit wrongdoing and accept blame. Unfortunately, none of these ads included words such as 'sorry' or 'apology.' Their effectiveness in driving customers back remains to be seen.

Governments in the U.S. and other countries might respond with existing tools – antitrust regulations, fines, forcing break up of big companies, etc. but there are questions about their efficacy. These industrial era tools of the 19th and 20th centuries have not kept pace with technological and data collection advancements of the 21st century. When a company is willing to pay a hefty price to buy another with no significant revenues, the trustbusters must be savvy to examine the dynamics of the transaction. Facebooks acquisition of WhatsApp for $16 billion was one such case when no red flags went up. Although, pre-acquisition scrutiny by the anti-trust regulators is infrequent, there are some instances of companies being fined for violating privacy policies. In 2013, Google was fined $7 million by a group of 37 states for collecting passwords and emails from unencrypted Wi-Fi networks its Street View cars connected to while passing by. The FCC fined Verizon $1.35 million in 2016 for violating consumer privacy by using 'supercookies' to track users' online whereabouts. While the FTC Act prohibits "unfair or deceptive practices," including lax data security policies, it can't assess penalties for violations and only enforce agreements with the companies to modify their practices and make promises for the future. (Duncan 2014).

In other countries, such as Germany, courts have repeatedly stepped in. A court in 2018 found five default settings and use of personal information by Facebook to be in violation of the consumer protection law (Hern 2018). Another instance stemming from a Spanish citizen's original "right to be forgotten" lawsuit, the Court of Justice of the European Union upheld the right in 2014. As a result of the ruling, Google and others have received over 600,000 requests to be forgotten from ordinary citizens, celebrities, politicians and other government officials (Doubeck 2018).

Momentum had been building in Europe since the eighties for tighter data privacy regulations and finally, the EU has taken a more forceful approach to protecting consumer data and privacy with the implementation of the GDPR. The evolution of European laws suggests they are more consumer-focused with privacy at the core. In the U.S. free speech is paramount and privacy protections are in the 'exceptions' category. While both seem valid for what they are intended to do, the results achieved in the age of the Internet might be varied (Wagner 2017).

In the U.S., data protections are implemented by a patchwork of regulations and enforcements through various federal and state agencies. For instance, the Federal Communications Commission (FCC) is tasked with regulations related to what data Internet Service Providers (ISPs) can or cannot sell.

The federal Health Insurance Portability and Accountability Act (HIPPA) deals with health care related consumer data. The Federal Trade Commission (FTC) enforces Children's Online Privacy Protection Act (COPPA) and also tries to get Instagram influencers to reveal their company/brand relationships. Also, in the U.S., the party in power tends to influence the regulations and their enforcements. Case in point, 'Net neutrality' provisions were removed in the wake of the recent political transition.

In Europe, albeit variations in regulations across industries, the basic principles had been agreed upon as being fundamental to their enforcement. Of course, Europe also sees some changes in the policies/enforcement with successive regimes. While U.S. is one country, the EU, made up of 28 countries, developed an agreement on the single supervisor or authority model. Similarly, U.S. consumers might blindly agree to a company's terms and conditions with the hope that their data is generally safe, Europeans have expectations as to limitations with company data use.

GENERAL DATA PROTECTION REGULATION (GDPR)

In this section, a brief genesis of the GDPR will be followed by a detailed discussion of its provision as it applies to marketers.

The origins of GDPR could be traced back to 1981 when a treaty for protection of individuals' data in automatic processing systems was signed and went into effect in 1985. At that time, 47 members of the Council of Europe ratified the treaty. Ten years later, the first European Data Protection Directive was enacted to protect the processing and movement of personal data. The same year, privacy was codified into human rights law for the first time. EU member states were required to implement the provisions of the law through national regulations by the end of 1998.

Ten or so years later, in 2009, EU discussions revolved around the impact of newer technologies and globalization with regard to use & protection of personal information and data exchange by governments, businesses and other entities. Globalization of data and cloud computing contexts were also being deliberated at that time. By the end of 2009, a "Future of Privacy" report was released at the behest of the European Commission (EC) and it emphasized better application of the then existing data protection principles and suggested the modernization of the legal framework. Based on further examination of personal data in the context of all policy areas including police & law enforcement, the Committee for Civil Liberties, Justice and Home Affairs (LIBE), the EC, in 2011 adopted a proposal regarding a comprehensive approach to personal data protection in EU countries that essentially led to the amendment of the Data Protection Directive of 1995. During the same year, at the 35th Privacy Conference of the German Association for Data Protection and Data Security (GDD), there was promulgation that the European Commission would implement a regulation to harmonize personal data protection laws in the EU.

In 2012, after a comprehensive review of the 1995 Data Protection Directive, a proposal for the General Data Protection Regulation (GDPR) to strengthen online privacy rights was recommended. A few amendments to the proposal were made in response to the U.S. trying to protect the interest of American companies operating in the EU. During the ensuing months, debates and discussions centered around enshrining it as directive or regulation, the definition of personal data, the concept of consent, etc. Finally, there was recognition that "a uniform and modern data protection law for the EU was needed to secure trust and generate growth in the digital single market," allowing EU citizens to maneuver through their digital life (Wilhelm 2015). During the same year, other revisions to the GDPR proposal were passed including increased sanctions/penalties, extraterritoriality provisions, limits for people profiling, third country data transfers, etc.

In 2014, the European Parliament overwhelmingly supported the GDPR by a wide margin and thus the provision could not be reversed. In the next two years, there were more discussions and machinations by law makers at the macro level with a view to developing the final version. There were more lobbying from business coalitions to remove certain provisions in the Regulation but the EU added an "anti-FISA" clause to the draft – this would essentially force business to deny personal data requests from non-member countries. In 2015, the U.S. warned that the GDPR could undermine efforts to track and share

information in terrorists attacks. During the same year, a common version of the Regulation was agreed to and was approved by various committees such as LIBE and other entities such as the European Council, European Parliament, and the European Commission. This final version of the Regulation included details on affirmative consent, about children using social media, right to be forgotten, right to know if personal data had been breached, plain language policies and penalties up to four percent of a company's worldwide annual revenue. An FAQ detailing the provisions and questions & answers regarding the GDPR were published (EUGDPR 2018).

In 2016, an action plan for the implementation of the GDPR was developed and published. During the same year the Regulation came into effect twenty days after its publication in the Official Journal of the European Union. In 2017, the European Commission proposed two new regulations on privacy & electronic communications and on the data protection rules as applied to EU institutions. Both of these were deemed consistent with provisions of the GDPR. After years of contemplation, discussions, and debates, the GDPR was formally effective from May 25, 2018. Approved by the EU Parliament in April 2016, the GDPR replaced the older 1995 Data Protection Directive (DPD) 95/46/EC and is designed to synchronize data protection laws across Europe, to protect and empower all citizens, and to reshape the way organizations approached the concept of data privacy (EUGDPR 2018).

So, in 2016, while Americans had their private and social media data hacked and potentially misused (Yahoo, Cisco, Oracle, LinkedIn, Wendy's, IRS, DOJ, Snapchat, etc), the European Union passed the General Data Protection Regulation with the express purpose of giving the residents more rights and control of their personal data collected by various commercial and non-commercial entities. The GDPR is the most significant influence on data privacy in decades. However, there is a 2-year post-adoption grace period after which the Regulation becomes fully enforceable throughout the EU. After that, there are various levels of fines and costs; the max includes fines up to €20 million or 4% of global turnover, whichever is higher. This figure does not include individuals' claims of liability for damages.

This regulation applies to all instances of processing personal data of EU citizens, regardless of the where the data processing takes place or where the company might be located or headquartered. The Regulation does not distinguish between paid or unpaid transactions, use of various devices/technology, etc. In other words, any entity with data on the continents' citizens will be affected. In order to implement the Regulation, the conditions for citizen consent have been toughened up. Companies can no longer hid behind incomprehensible "terms and conditions" and they are now required to make it clear using plain language, distinguishable from other information and easily accessible. They must also allow the citizens to easily withdraw their prior consent.

Key Principles of the GDPR

The Regulations apply to all EU citizens regardless of purchase status. In other words, the focus is on how the sites/companies target them and how their data is used not how they are using a company site (Data Services Inc. 2018). Article 5 of the Regulation outlines seven key principles that form the core of the data protection regime (ICO 2016). They relate to (a) lawfulness, fairness & transparency; (b) purpose limitation; (c) data minimization; (c) data accuracy; (e) data storage limitations; (f) data integrity & confidentiality; and (g) accountability. Brief descriptions of each of the principles as it relates to EU citizens' personal data are provided below (ICO 2016).

1. Personal data should be processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Data collected for specified, explicit and legitimate purposes should not be further processed in a manner that is incompatible with original purposes. Additional processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is not be considered to be incompatible with the initial purposes;
3. Data collection need to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. Collected data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data are correct for the purposes for which they are processed. Inaccurate information should be erased or rectified without delay;
5. Data need to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
6. Data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures;
7. The controller (i.e., the company holding the data), is responsible for, and be able to demonstrate compliance with the principles by having appropriate processes and records. According to the provisions of the GDPR, the "controller is the entity that determines the purposes, conditions and means of processing of personal data" (EUGDPR 2016).

These principles embody the spirit of the Regulation and form the basis of the entire regulatory framework. A positive mindset toward the Regulation might allow traditional and 'Net based companies to build and implement better data protection systems not only for EU citizens but for all customers worldwide. Based on these principles, the GDPR provides for individual European citizens to take control of their personal data through certain "assigned" privacy right as outlined below:

1. *The Right to be informed:*
   When businesses collect data, they should reveal what personal data is being collected, how/what they are going to use it for, how long would they store it and with which organizations would they be sharing the data. Also, all data breach notifications are mandatory within 72 hours of awareness in all member countries especially if it is likely to "result in a risk for the rights and freedoms of individuals" (EUGDPR 2018). Third party processors (ex. Equifax) are required to notify their customers (ex. Visa) of such breaches in a reasonable time.
2. *The Right of Access:*
   EU citizens have the right to contact businesses to access their personal data held in an electronic format without payment. This includes the nature and type of data being stored, what it is being used for and details of sharing with other parties.
3. *The Right to Rectification:*
   By accessing the personal data held by companies, EU citizens have the right to ensure that the information is accurate and have it corrected if found to be false or inaccurate.
4. *The Right to Erasure:*
   Citizens have the 'right to be forgotten' or have their personal data erased from businesses and data processors. Once the right is invoked, the dissemination of such data will need to cease. Businesses, however, can weigh the request for erasure with the public interest in the availability of such data. Thus, this is not an absolute right and thus, a business can refuse do comply under the right circumstances.
5. *The Right to Restrict Processing:*
   Similar to #4, citizens can deny consent for data processing by an organization whether or not consent was given in the past. Again, the business should inform the person about what it is doing with the data to help with the consent-no consent decision. Similar to #4, this right is not absolute.
6. *The Right to Data Portability:*
   This includes the right of people to receive data and transmit it in a commonly agreed upon portable electronic format and take that to another organization. An example of this could be

personal data that can be downloaded from Facebook or Google but they would have to be in a compatible format.

7. *The Right to Object:*
   If a consumer finds their personal data being used in a manner that they are opposed to, then they can demand business to cease. For instance, using data to send promotional literature or make telemarketing calls without consent.
8. *The Rights regarding Automated Data Processing and Profiling:*
   Profiling and targeting using automated systems can be objected to and appealed against if such decisions by businesses affect the citizen. Therefore, decisions regard credit, job application, etc., that have legal consequences are affected. Explicit and informed consent is required in these situations.

According to MacDonald (2018), one of the main impetuses for the introduction of new data protections regulation was the existing privacy framework was based on the legacy 1980 directives, although later amended. The legacy rules were basically directives (not regulations) and became outdated given the use of newer technologies including social media, artificial intelligence, cloud computing, etc.

IMPLICATIONS FOR MARKETERS

A survey by HubSpot found that only 36 percent of marketers have heard of the GDPR and about 15 percent have done little to prepare, thereby risking non-compliance (HubSpot 2018). According to another study, four weeks before the deadline, only 28% of the businesses considered themselves fully compliant while about 47% were confident that they would comply by the deadline (Marketo 2018). The conscientious marketer/business will probably use this opportunity to engage with their customers in a manner that respects the intent of the Regulation and beyond. Companies that are at the opposite end of the compliance spectrum are likely to be surprised by the seriousness of the enforcement. Within hours of the implementation, complaints have been filed against Facebook, its properties, and Google to the tune of $8.8 billion. These complaints, submitted to the Data Protection Authority, allege lack of free consent in accessing the companies' sites (Tsakiridi 2018).

All the rights granted EU citizens have a significant impact on how marketers go about their business of collecting, processing, disseminating data and targeting consumers. Use of algorithm-based decisions will be restricted once consumers are given control of their digital lives. For instance, if a car loan is denied based on automated or algorithmic decisions, the consumer has the right to challenge the decision, demand human intervention and also "insist on regular audits of those algorithms" (New York Magazine 2018). Sure, marketers will test the limits of the law and strategize how they can get away with few changes that are not likely to disrupt their business-as-usual model.

Customer facing companies with existing relationships (ex. Facebook, Google, Amazon, Apple, etc.) might find the fixes fairly simple but the back end processers that help facilitate behavioral targeting (ex. doubleclick, pushcrew, etc.) need to obtain explicit consumer consent to ply their trade. Some companies might find it difficult to comply. For instance, unroll.me, the company that helps declutter the email inbox, has decided not to do business in the EU. Incidentally, unroll.me faced backlash in the US for scouring email data to sell to companies like Uber in order to keep tabs on Lyft. The CEO apologized for this indiscretion (NY Times 2018).

Given the dawn of the GDPR era, businesses face a choice with regard to implementation of marketing practices in EU and beyond. One strategy entails the implementation of the GDPR compliant model for EU and another 'business-as-usual' model for the rest of the world. But given the global nature of business and the Internet, this might be a cost-prohibitive proposition. A second strategy, as proposed by companies such as Facebook, is to extend GDPR protections to all users, if they opt-in. It is likely that the Cambridge Analytics scandal that tainted the company right before the GDPR implementation might have had some influence on their thinking.

All marketers and businesses are likely to be affected if they have a need to collect personal data. At the risk of oversimplifying the regulatory impact on marketing, one can envision the impact in three

specific areas – data collection & permissions; data storage & processing; and termination of customer relationships. Researchers have focused on these areas in a variety of ways (MacDonald 2018).

First, data collection and permissions are about managing transparency, opt-ins, and providing justification for specific data collection. Companies (controllers of data) should be transparent in their efforts and provide users, in plain language, the details in order for them to make an "informed, specific, unambiguous and revocable" consent. For instance, customers and prospects need to provide express consent to receive promotional materials. Companies cannot assume opt-in with pre-checked boxes on the site and they should allow customers to make a deliberate choice and explicitly provide permission to be contacted or receive a newsletter. At the same time, only data that is required, relevant, and limited to, say convert a prospect to buyer, can be collected – nothing more. Instead of sweeping up data that might or might be needed, one has to be more focused on the needed information. For instance, appliance manufacturers in the past asked for "irrelevant" information when making customers fill out the warranty cards. Asking where the treadmill was bought might relevant but information about customers' food preferences might be unwarranted.

Second, data storage and processing is about making sure that only needed data is held and used for its original purpose. EU citizens can ask to verify the accuracy of the data and thus will have the ability to correct outdated or incorrect data. Security of the data is also of paramount importance under the Regulation. Companies/controllers need to utilize appropriate technological and security measures to protect it from being breached or hacked. So encryption, anonymization or pseudonymization and detaching data from other less secure systems are critical. Also, accountability for this function lies with the business/controller. The Controller needs to document and prove compliance by developing appropriate processes & procedures.

Third, the ultimate step a company or a consumer can take is to terminate the interaction/ relationship with a business. EU citizens' now have the right to be 'forgotten' by all entities in the data value chain. However, there are provisions in the Regulation for not deleting the data if it is warranted by other public interest considerations. There has been multiple ruling regarding the right to be forgotten prior to the implementation of the GDPR. For instance search engines were ordered to remove affected results. Marketers now have to make the data easily accessible and provide options for removal beyond having a 'unsubscribe' link within email marketing template. While many email subscription marketers already do so, a study found that a small percent of them did not contain the link (MacDonald 2018).

Given the topical nature of these new requirements from the EU, there is no dearth of articles and sites that recommend effective compliance policies for general marketers and for those involved in mobile marketing, email marketing, telemarketing, etc. The Web is also brimming with consultants offering strategies, FAQs. checklists, kits, etc., to help companies become compliant.

GENERAL ASSESSMENT OF GDPR

While the basic idea behind the implementation of GDPR is consumer data and rights protection may be noble, it might create significant issues for businesses and marketers interacting with EU customers. Coincidently, there have been some unfavorable assessments of the GDPR as developed and implemented by the EU. The basic culture of the Internet has been wary of national/boundary sovereignty and many have argued against anything that harms the freedom of the network. GDPR is more about the network user sovereignty within a certain bounded area.

Firstly, some estimates put the price tag for preparation and compliance at about $7.8 billion (Bloomberg Businessweek 2018). It is argued the large companies can afford higher cost of compliance while smaller businesses might suffer. Start-ups, without strong financial backing, are more likely to be affected. According to the Interactive Advertising Bureau (2018), digital advertising adds $625 billion to EU's economy and GDPR implementation will raise the cost of doing business since data-driven advertisements are "worth three times as much as non-targeted ads" (New York Magazine, 2018). Of course, another way to look at this is to realize that advertisement-dependent model might eventually give way to subscription-based models such as Netflix, Spotify, Amazon Prime, etc. In a study published

earlier, eight-seven percent of businesses surveyed had difficulty estimating the cost impact of the regulation and slightly lower percentage could not quantify their spending on consumer data protection (Deloitte 2013).

Secondly, laws and regulations don't always keep up with technology, and GDPR might not be an exception with regard to blockchain technologies. Some predict that blockchains as currently programmed might be incompatible with GDPR (The Ledger 2018). It is likely that the technology might have to be redesigned to allow its co-existence with the new EU law. Some have expressed concerns about how GDPR might handle Artificial Intelligence and Machine Learning paradigms (Wachter, Mittlestadt, and Luciano 2017). Can the right to receive an explanation or justification for decisions and the right not to be subject to automated decision making make the implementation of some of the provisions difficult?

Thirdly, there is concern that GDPR might make Web surfing experiences more cumbersome given the policy to obtain consent at every stage. Consumers might have to make a trade-off between privacy and convenience. If not, they might flood companies with requests for personal data held by them. Although, pre-GDPR, EU citizens had the right to request the nature/type of personal data companies stored, they have now have the right to have the data deleted and companies have to respond within a month of request (Ismail 2018).

Finally, there are concerns about how users and consumers will act to take advantage of the provisions of the GDPR. Some question whether consumers are ready, willing and able to do so. If not, the GDPR efforts are bound to fail as consumers lose interest (Koops 2014).

DISCUSSION

The CEO of Sun Microsystems, Scott McNealy, once famously stated that people need to get over privacy concerns since there is none in the technology era. The EU would beg to differ. Albeit the proclamation of business cataclysm as the result of GDPR, analyses show that the field of marketing, specifically data-based marketing, will undergo significant changes but not be doomed. The requirements might revolutionize how companies deal with personal information and in this regard, the Regulations set a higher standard for marketers in their dealings with prospects and customers. Marketers will be forced to respect customers' personal data and provided greater transparency in the collection, processing, and deletion of the information.

If viewed from a customer-centric perspective, GDPR requirements could be one of the major drivers of system design rather than an afterthought. It is imperative that marketers design their data collection/processing/storage/deletion regimes not just to meet the letter of the law but the overall spirit of the Regulation. Adjusting to the new realities is likely to provide marketers an opportunity to set the record straight with consumers with regard to their data and how it is monetized. There should be a trade-off. Data allows customers to be targeted with custom four-Ps that might or might not appeal to them but companies monetize valuable customer data that they essentially obtain for free minus data collection costs.

Also, effects of the Regulation will be felt beyond the EU in two ways. Firstly, companies complying with the Regulations might implement the same data strategies in other regions/countries. Facebook announced that it will implement some of the provision of the Regulations for customers outside the EU (Kelly 2018).

Secondly, the success of the GDPR might prompt other countries to adopt or modify it to suit their cultures. Israel, New Zealand, Argentina, Japan, Columbia, South Korea and others have either completed or are in various stages of assessing and updating their data protection programs, sometimes adopting GDPR verbatim (Scott and Cerulus 2018). Back in the U.S, there is a ballet initiative in California regarding personal data collection. It seems to go beyond GDPR by expanding the definition of personal data to include olfactory, psychometric data, and encompasses inferences drawn from raw data (Uehlein 2018). The language used here seems to concern marketers. Hopefully, the GDPR is good preparation for facing governance elsewhere.

REFERENCES

Bloomberg Businessweek (2018). *The Wrong Way on Data*. Retrieved May 20, 2018, from https://www.scribd.com/article/378853136/The-Wrong-Way-On-Data

Brelend, A. (2018). *Americans Want Tougher Regulations for Tech Companies: Poll.* Retrieved March 03, 2018, from http://thehill.com/policy/technology/384144-poll-americans-want-tougher-regulations-for-technology-companies

Cakebread, C. (2017). *You're Not Alone, No One Reads Terms of Service Agreements*. Retrieved March 23, 2018, from http://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11

CitizenVox (2018). *Public Citizen Finds Widespread Support for Regulating Big Tech Companies and Protecting Data Privacy*. Retrieved May 25, 2018, from https://www.citizenvox.org/2018/05/24/public-citizen-finds-widespread-support-for-regulating-big-tech-companies-and-protecting-data-privacy/

Comcowich, W. (2018). *How Effective is Splashy Apology Ads from Facebook, Uber, and Wells Fargo?* Retrieved June 03, 2018, from https://glean.info/how-effective-are-splashy-apology-ads-from-facebook-uber-wells-fargo/

Crosby, L. (2016). *How Easily Do Customers Forget? When Transgressions Against Them Are Poorly Remediated. The Memory Can Be Difficult To Dismiss*. Retrieved May 23, 2018, from https://www.ama.org/publications/MarketingNews/Pages/cost-customer-trust-violations.aspx

Data Services Inc. (2018). *EU Data Regulation – Here Comes GDPR*. Retrieved May 22, 2018, from http://www.dataservicesinc.com/newsletter/eu-data-regulation-here-comes-gdpr/

De Pinto, J. (2018). *Americans are Skeptical Facebook Can Protect User Data*. Retrieved May 20, 2018, from https://www.cbsnews.com/news/americans-are-skeptical-facebook-can-protect-user-data-cbs-news-poll/

Deloitte (2013). *Economic Impact Assessment of the Proposed European General Data Protection Regulation: Final Report*. Retrieved March 19, 2017, from deloitte-uk-european-data-protection-tmt.pdf

Doubek, J. (2018). *Google Has Received 650,000 'Right to be Forgotten' Requests Since 2014*. Retrieved March 01, 2018, from https://www.npr.org/sections/thetwo-way/2018/02/28/589411543/google-received-650-000-right-to-be-forgotten-requests-since-2014

Duncan, G. (2014). *Can the Government Regulate Internet Privacy?* Retrieved December 10, 2017, from https://www.digitaltrends.com/web/government-warn-us-data-breaches/

EUGDPR (2018). *GDPR Key Changes*. Retrieved May 15, 2018, from https://www.eugdpr.org/

EUGDPR (2016). *GDPR FAQs*. Retrieved March 22, 2018, from https://www.eugdpr.org/gdpr-faqs.html

Hale, T. (2017). *How Much Data Does The World Generate Every Minute?* Retrieved May 28, 2018, from http://www.iflscience.com/technology/how-much-data-does-the-world-generate-every-minute/

Hart, J. (2018). *Data Breaches Are Taking a Toll on Customer Loyalty*. Retrieved March 23, 2018, from https://www.csoonline.com/article/3250836/data-breach/data-breaches-are-taking-a-toll-on-customer-loyalty.html

Hern, A. (2018). *Facebook Personal Data Use and Privacy Settings Ruled Illegal by German Court*. Retrieved March 01, 2018, from https://www.theguardian.com/technology/2018/feb/12/facebook-personal-data-privacy-settings-ruled-illegal-german-court

HubSpot (2017). *What is the GDPR? And What Does it Mean for the Marketing Industry?* Retrieved April 13, 2018, from https://blog.hubspot.com/marketing/what-is-the-gdpr

Hubspot (2018). *Facebook Has Suspended 200 Apps in Data Misuse Audit*. Retrieved May 16, 2018, from https://blog.hubspot.com/marketing/facebook-suspends-200-apps-data-misuse-audit

ICO (2016). *GDPR: The Principles*. Retrieved Mar 23, 2018, from https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

Ismail, N. (2018). *UK Organizations Should Expect to be Overwhelmed by Data Privacy Requests Following GDPR's Deadline*. Retrieved May 15, 2018, from http://www.information-age.com/post-gdpr-data-privacy-requests-123471786/

Jacob, D. (2017). *3 Takeaways from the 2017 Cost of Data Breach Study*. Retrieved January 14, 2018, from https://www.propertycasualty360.com/2017/07/05/3-takeaways-from-the-2017-cost-of-data-breach-stud/?slreturn=20180508173633

Janrain (2018). *Cambridge Analytica Breach Draws Shift in Consumer Attitudes Toward Privacy*. Retrieved May 13, 2018, from https://www.janrain.com/company/newsroom/press-releases/janrain-survey-cambridge-analytica-breach-draws-shift-consumer

Kelly, H. (2018). *Facebook will Push Privacy Alert to Users Outside EU Ahead of GDPR*. Retrieved April 01, 2018, from http://money.cnn.com/2018/05/24/technology/facebook-gdpr-us/index.html

Koops, B.-J. (2014). The Trouble with European Data Protection Law. *International Data Privacy Law*, 4(1 November), 250–261.

MacDonald, S. (2018). *GDPR for Marketing: The Definitive Guide for 2018*. Retrieved June 05, 2018, from https://www.superoffice.com/blog/gdpr-marketing/

Marketo (2018). *Marketo and the General Data Protection Regulation (GDPR)*. Retrieved May 24, 2018, from https://www.marketo.com/company/trust/gdpr/

Marketo (2018). *The Hardest Part About GDPR Isn't What You Think*. Retrieved May 24, 2018, from https://blog.marketo.com/2018/05/hardest-part-gdpr-isnt-think.html

McKinsey & Company (2016). Monetizing Car Data: New Service Business Opportunities to Create New Customer Benefits. *Report on Advanced Industries*, (September). Retrieved from https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Monetizing%20car%20data/Monetizing-car-data.ashx

New York Magazine (2018). *The EU's New Privacy Laws Might Actually Create a Better Internet*. Retrieved May 20, from http://nymag.com/selectall/2018/05/can-gdpr-create-a-better-internet.html

New York Times (2017). *Unroll.me Service Faces Backlash over a Widespread Practice: Selling User Data.* Retrieved May 15, 2018, from https://www.nytimes.com/2017/04/24/technology/personal-data-firm-slice-unroll-me-backlash-uber.html

Obar, J. A., & Oeldorf-Hirsch, A. (2016). *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*. The 44th Research Conference on Communication, Information and Internet Policy (August 24). Retrieved from https://ssrn.com/abstract=2757465

Perez, E. (2013). *NSA: Some Used Spying to Snoop on Lovers*. Retrieved November 14, 2017, from https://www.cnn.com/2013/09/27/politics/nsa-snooping/

Ryoo, J. (2016). *Big Data Security Problems Threaten Consumers' Privacy*. Retrieved January 3, 2018, from https://theconversation.com/big-data-security-problems-threaten-consumers-privacy-54798

Santarcangelo, M. (2016). *What Research Reveals About Consumer Behavior After a Security Breach*. Retrieved May 15, 2018, from https://www.csoonline.com/article/3026578/leadership-management/what-research-reveals-about-consumer-behavior-after-a-security-breach.html

Seetharaman, D., & Grind, K. (2018). *Facebook Gave Some Companies Special Access to Additional Data About Users' Friends*. Retrieved June 9, 2018, from https://www.wsj.com/articles/facebook-gave-some-companies-access-to-additional-data-about-users-friends-1528490406?mod=hp_major_pos16?mod=djem_jiewr_BE_domainid

Scott, M., & Cerulus, L. (2018). *Europe's New Data Protection Rules Export Privacy Standards Worldwide*. Retrieved March 18, 2018, from https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/

Seeking Alpha (2018). *Tesla Vs. Ford Vs. GM: Earnings Roundup For The 3 Major U.S. Automakers*. Retrieved May 29, 2018, from https://seekingalpha.com/article/4146407-tesla-vs-ford-vs-gm-earnings-roundup-3-major-u-s-automakers

Shane, S., Perlroth, N., & Sanger, D. (2017). Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core. Retrieved January 14, 2018, from https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html

Siliconrepublic (2018). *What are the Compatibility Issues Between GDPR and Blockchain*. Retrieved May 24, 2018, from https://www.siliconrepublic.com/enterprise/blockchain-gdpr-eu

The Conversation Blob (2018). *What Does GDPR Mean to Me? An Explainer*. Retrieved May 20, 2018, from https://theconversation.com/what-does-gdpr-mean-for-me-an-explainer-96630)

The Ledger (2018). *The Blockchain-GDPR Paradox*. Retrieved May 24, 2018, from https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047

Tsakiridi, S. (2018). *First Complaints Under the GDPR Lodged Within Hours . . .* Retrieved June 1, 2018, from https://privacylawblog.fieldfisher.com/2018/first-complaints-under-the-gdpr-lodged-within-hours

Uehlein, M. (2018). *Advertising and Marketing Industry Aligns on Reckless California Data Initiative*. Retrieved June 17, 2018, from https://thedma.org/blog/data-driven-marketing/advertising-marketing-industry-aligns-reckless-california-data-initiative/

Wachter, S., Mittlestadt, B., & Floridi, L. (2017). Why a Right to Explanation of Automated Decision Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(1 May 2017), 76–99.

Wagner, T. (2017). *The Main Differences Between Internet Privacy in the U.S. and the EU*. Retrieved September 03, 2017, from https://www.marketplace.org/2017/04/20/tech/make-me-smart-kai-and-molly/blog-main-differences-between-internet-privacy-us-and-eu

Wilhelm, E.-O. (2016). *A Brief History of the General Data Protection Regulation*. Retrieved February 17, 2018, from https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/