Investigating GDPR Compliance across Consumer-Related Websites: Are Businesses Telling Consumers the Truth About Data Collection?

Sabrina Fang
Mike Yao

Abstract
The project aims to examine the compliance of GDPR among websites of various sectors. By doing a content analysis on selected websites of Fortune 500, various patterns emerged for complying with the regulations. The majority of websites do not inform users of data collection. Most websites adopt communication strategies that inform users of data collection but withhold the rights to opt out. Few websites truly obtain consent and give consumers the option to opt out before data collection. We categorized all the websites into groups of full compliance, partial compliance, and non-compliance. In addition, some businesses have been found to adopt global strategies that only comply with GDPR when users are identified as EU citizens. Lastly, we give provide some recommendations with regards to how businesses could comply with GDPR.

Keywords
Consent; Data collection; GDPR; Privacy; Consumer.

Introduction

General Data Protection Regulation (GDPR) has come into full effect since May 25, 2018. Implemented by the EU, the regulation is designed for protecting EU citizen's data and privacy from data breaches. It is a new regulation designed to protect web users' privacy and personal information, replacing the 1995 Data Protection Directive which gradually becomes incompatible in the digital age. Within the framework of GDPR, pivotal impacts have been observed from consumers to businesses and any entities that process personal information.

In the data-driven world, collecting personal data has become an efficient way of delivering advertising (Glass & Callahan, 2015). From a consumer perspective, personal data is now handled more cautiously with the enforcement of GDPR. With regards to the control of personal data, a new balance between consumers and businesses is introduced. Consumers are granted more rights in controlling their own information, including the right of not divulging any personal data to businesses. On the other hand, businesses are allowed to collect and process personal data only if consumers consent to the term. Failure to comply with the regulations may result in an enormous fine of up to €20 million.

To meet the requirements of GDPR, websites are making changes to their privacy policy. Studies have shown that GDPR has led to a 4.9% increase in the provision of privacy policies by websites and 16% more websites are presenting cookie consent notices (Degeling, Utz, Lentzsch, Hosseini, Schaub, & Holz, 2018). However, while notable changes have been made with regards to privacy rights, not all companies are following the regulations months after GDPR went into full enforcement. Research has indicated that GDPR compliance has yet to be improved. TrustArc (2018) has revealed that one month after the GDPR went into enforcement, only 20% of companies believed that they are fully compliant with the regulations. Additionally, compliances were not consistent across the globe despite GDPR's extraterritorial effect. While 27% of EU companies believed compliances are achieved, only 12% of US companies did the same.

The goal of the project is to examine how businesses comply with GDPR. We investigated websites' GDPR compliances from a consumer perspective by conducting a content analysis of websites from various sectors and brands that are related to consumers. We sought to find out the user experience when browsing and whether differences exist for users across different regions.

Literature Review

The enforcement of GDPR is expected to bring significant impacts for both businesses and consumers. Businesses are affected for its strict regulations on data collection. Sixty percent of professionals in the industries have expected drastic changes which GDPR will bring to the organizations' workflow of data collection (Ponemon Institute, 2018). The advertising industry, for instance, will be influenced due to the growing trend in digital advertising which relies on personal data. In 2017, the market of global digital advertising grew 21% to 88 billion (PwC, 2018). In the U.S, the total spending of digital advertising accounts for 40% of all ad spending (McNair, 2018). While the collection of personal data has encouraged the growth of digital advertising, advertisers and third-party companies that process personal data are now being regulated by GDPR, resulting in sweeping changes in strategies and tools used in the advertising industry.

Data Collection and Cookies Placement under GDPR

The use of cookies, for example, has generated heated discussions under the framework of GDPR. Cookies are small files that are stored locally on people's computer.

The number of third-party cookies on news websites are reported to have decreased by 22% in Europe since the enactment of GDPR (Libert, Graves, & Nielsen, 2018). Cookies can track people's browsing history and preferences which can generate valuable insights based on people's activities on the web. They are often placed by either business themselves or third-party companies for analytical processing. Data collected by cookies is useful for online advertisers and marketers because cookies are essential indicators in helping them place their ads on the internet. Behavioral advertising and retargeting ads, for example, rely on third-party cookies that help advertisers track consumers across multiple devices and build consumer profiles, creating messages that target to consumer interests more accurately. Additionally, real-time bidding, an approach through which online advertising is sold and bought, also relies heavily on consumer data and insights because through which bidders can automatically bid for an ad to deliver personalized ads that cater to individual preferences.

While the technology has become a prevailing strategy for marketing and advertising industries, the use of tracking cookies is regulated by GDPR because cookies can be identifiers of web users. According to Article 4 of GDPR, when data can identify either directly or indirectly at someone, it is considered personal data and falls under the regulation of GDPR. This is an indication of how the concept "privacy" is evolving, as manifested by the articles of GDPR. Within the framework, the scope of personal data has extended beyond explicit data that consumers choose to disclose themselves, including personal data like home address, phone number, and credit card number, etc. Information disclosure on the internet, from a consumer's point of view, has advanced from data sharing to data being taken. Since placing tracking cookies has become one of the main approaches in online advertising, how businesses and advertisers comply with GDPR is an important issue.

Consent

By complying with GDPR, businesses are required to obtain consent for data collection. GDPR protects consumers by giving consumers more rights while putting more obligations on businesses. Consumers are having more control of their personal data under the framework of GDPR. Responsibilities now lie on the businesses to obtain consumers' consent before collecting personal data and provide transparent information to the consumer. To meet the requirements, the approach of using privacy banner as a communication strategy is widely adopted. After the enforcement of GDPR on May 2018, the first and foremost change that impacts the user experience of internet browsing must have been the flux of privacy banners on websites of various brands. In general, privacy banner should be a bridge for communication. It serves two purposes, obtaining consent for data collection and providing information to consumers, which corresponding to two of the GDPR principles: lawful and transparency.

Consents are one of the legal bases for the processing of personal data to be lawful. The GDPR mandates that for a consent to be valid, the consent must be "freely given, specific, informed and unambiguous indication of the data subject's wishes." Moreover, consent should be provided with a clear, affirmative action. However, research has shown that obtaining consent as the legal basis for data processing has been challenged for privacy engineering. Schiffner et al. (2018) argued that business will be pushing users for giving consent so that all the data processing will meet the requirements of GDPR while striving to meet the requirements stating that consent should be in "intelligible and easily accessible form, using clear and plain language," as

referenced in Article 7. Therefore, we would first like to find out:

RQ1: Are companies complying with GDPR by obtaining consent before data collection?

While privacy banner should be serving its purpose of informing consumers of data collection and being transparent, research has shown otherwise. A research done by Kulyk, Hilt, Gerber, and Volkamer (2018) indicates that users tend to close the banner without understanding the messages or ignore the existence of such banners. Obara and Oeldorf-Hirsch (2018) outlines that consumers tend to ignore privacy policy when registering for social networking services. This indicates that consumers tend to focus more on achieving their goals without allocating cognitive resources to information that is irrelevant to the goals or information that may be disrupting to the browsing experience. From a consumer perspective, ignoring the privacy banner and stay inactive on the site does not necessarily mean consenting to the data collection. It merely suggests that consumers are paying less attention to the additional task of giving consent. Given that GDPR mandates "silence, pre-ticked boxes or inactivity should not therefore constitute consent," businesses should provide opt-out options of data-collection to consumers. Consumers have the right to not share their personal information with the businesses. Upon giving consent, consumers are also endowed the right of withdrawing consent at any time. Yet, a recent study has demonstrated the diverse use of privacy banners does not necessarily meet the requirements of GDPR. Dangeling et al. (2018) outlines the five predominant types of privacy banners were identified with how users give their consent. The types include banners with no options of opting out data collection, confirmation-only banners, banners with binary options, slider-based banners, checkbox banners and other types of banners. Companies differ in how they comply with GDPR, creating different types of banners in being transparent and lawful. The research indicates that there are various strategies in gaining consent. Thus, we would like to delve further into the strategies used on websites. We raised the question:

RQ2: How do companies obtain consent via privacy banners?

Transparency

Transparency under the principle of GDPR indicates that businesses should be transparent about how they process personal data. Users should have access to their own data and they should be informed of the rights with regards to their personal data. Article 12 of GDPR requires companies to inform the data subject of the data processing, and the information must be presented with clear and plain language with an easily accessible form. Henceforth, from a business perspective, it is necessary for them to balance between providing transparent information and keeping the information in clear and plain languages (Schiffner et al., 2018).

Transparent information can be provided using privacy banners. The advantage of using privacy banners includes the creation of a straightforward user experience. Consumers don't have to click around seeking for information; instead, they can access the information through where they landed. However, the struggles remain for putting all the information regarding data collection on a piece of a small pop-up banner. From the perspective of consumers, providing transparent information on a pop-up banner can introduce two possible outcomes: more information for the leverage of granting consent or more hindrance to the user experience. In accordance with the GDPR, users should have access to transparent information with regards to how their data is collected, processed and stored. Article 13 lists the information that data subject should have access to, including contact information,

purposes of data processing, legal bases for the processing, and the rights of the data subject. The rights of data subject include but not limited to the right to access, rectify, delete personal data. Furthermore, data subjects should also be granted the right to portability, the right to object data processing, and the right to revoke consent. The dilemma of providing every detail on a banner could lead consumers into making trade-offs on information processing, paying attention only to the selected parts of information (Morris, Mazis, and Brinberg, 1989). Thus, businesses are providing transparent information through both putting up a full privacy policy and updating their existing ones. Increases in average word count and average reading times of privacy policies for some of the top websites in the US including eBay, Netflix, Wikipedia have been reported after the implementation of GDPR (Sobers, 2018). The same report also suggests that an increase in comprehension levels is found for reading privacy policies.

Besides struggles described above, other obstacles exist for following the transparency principle in practice. The right to withdraw consent has caused prolong controversy. More precisely, the practicality of web users exercising the right to be forgotten (article 17) is met with technical issues because it involves knowing all the controllers that process data and where all copies of data are stored in relevant parties. Upon knowing all the processors, the additional obligation to inform them of the erasure request puts extra burdens on the controllers. While the right plays an integral role in the GDPR, the erasure undoubtedly takes effort, time, and money to locate all the data, and still, it remains questionable as to whether the data has been successfully deleted from all sources (Politou, Alepis, and Patsakis, 2018; Tjong Tjin Tai, 2016). In fact, the right to be forgotten has been surveyed to be one of the most concern articles among the regulations, with over 50% of the companies express their concern for implementing (Cybersecurity Insiders, 2018).

Additionally, it is also proposed that the right to be forgotten would ultimately result in the loss of information due to "*preventive actions like anonymization of database per default*" (Malle, Kieseberg, Weippl, & Holzinger, 2016). From the perspective of data backup and archive, the right to be forgotten imposes challenges in practice. Backup is a continual plan for businesses which ensure a quick recovery from hardware failures and system crashes. The controversy raises with regards to whether the right to erasure personal data applies to back up as well for data backup is a repeated process of data storage (Politou et al., 2018).

RQ3: How do websites comply with the transparency principle while balancing with user experience?

Challenges in Complying with GDPR

Prior to the enforcement of GDPR in May 2018, several reports have revealed how industries were coping with the regulations. According to research done by Ponemon Institute (2018), which surveyed over 1000 companies, almost half of the companies expressed that they were not ready to comply with GDPR and that they will not meet the deadline by May 2018. Besides limited time of preparation and the need to make comprehensive changes (Ponemon Institute, 2018), the lack of expert appears to be one of the main barriers in achieving full compliances. Both US and UK professionals have low confidence in meeting the deadline and have expressed concerns for following the requirements of GDPR. Professionals indicate that helps are most needed in developing a GDPR plan (TrustArc, 2018). Eighty-six percent of professionals said that GDPR is more difficult or equally difficult than other privacy regulations, and they express that the path to compliance is complex (Ponemon Institute, 2018). In addition, 25% of professionals have limited knowledge or no

knowledge of GDPR (Cybersecurity Insiders, 2018). As suggested, businesses are stymied due to the lack of sources, and it's worth the examination of how these obstacles reflect GDPR compliances across different regions.

Impact on User Experiences of Different Regions

Geographically, while GDPR is enacted by EU, the potential impact of the regulation extends beyond. One of the challenges posed by the GDPR is the compliance in a "*worldwide context in which those who control and process personal data are often from legal and social cultures different from those of the EU*" (Schiffner et al., 2018). All businesses that use personal data to reach out to their consumers are now under the regulation of GDPR. Regardless of company location, GDPR is applicable to any company that processes personal data of EU citizen. In fact, companies are worried that failure to comply with GDPR will bring negative impacts to their global operations (Ponemon Institute, 2018). It's apparent that companies outside of EU have been affected by the regulation as well. However, while it has been acknowledged that GDPR has an extraterritorial effect, it's worth noting that businesses across the globe have demonstrated different levels of preparations. Before GDPR came to live, it has been brought to light that EU businesses have reported a higher level of readiness than US businesses, and they are more prepared to respond to data breach incidents as well. Additionally, more EU businesses have conducted data audits than US businesses (Ponemon Institute, 2018). The research is in accordance with the compliance after the enforcement. A GDPR compliance report made by Reuters Institute (2018) indicates that European news websites are responding to GDPR either by obtaining consent or decreasing the use of cookies. It has been revealed that after the enforcement of GDPR, there is a 22% drop in the number of third-party cookies usage across news websites, including advertising cookies and social media cookies. Meanwhile, the same report highlights the fact that US-based technology companies, including Google and Amazon, remain high levels of cookie usage.

Before GDPR's full enforcement in May 2018, businesses are granted a two-year preparation period after its adoption in 2016. However, instead of updating companies' policy on privacy, news reports have shown that there are top companies and news websites in the US take strategies otherwise. There are US websites that block EU web visitors from entering (Moses, 2018). This blocking strategy indicates that not all companies are willing to or not fully ready for complying with the regulation and that there are other approaches to take besides obtaining consent from their users. Therefore, it is crucial that we get a deeper understanding of the strategies when facing visitors from EU as well as other places in the world. Taking a global perspective, we wanted to observe the user experiences of people from different places and examine that whether they would get the same experience of browsing the site. We take an in-depth look on consumer experience to see if there is a discriminating service against EU users.

> **RQ4:** Is there consistency in how companies enforce their privacy policy for visitors from different places?

Method

The project aims to discover how companies comply with GDPR. In the current project, we conducted a content analysis on websites from around the world. We chose the United States, Germany, and Singapore as our three main locations for the analysis. We chose Germany because it is a country in the EU and it is also the first member state to enact GDPR, and Singapore due to its reputation as a country of strict rules on privacy in Asia. In order to access the websites from perspectives of different countries, we used Windscribe, a VPN provider that allowed us to visit websites

using IP addresses from different countries.

Sampling Strategy

The population for the project was drawn from the list of "Fortune Global 500" in 2018. Fortune Global 500 is a list that ranks the revenue of the top 500 companies in the world. In 2018, the companies that made the list generated $30 trillion in revenues. The list of companies is categorized into 23 sectors and represent 33 countries. We selected 5 sectors that are most relevant and the most representative to consumers in their daily lives as our sampled data, including apparel, food and drug store, retailing, technology, and transportation sectors. In sum, a sample of 74 companies was selected from the list (See appendix 1).

Some companies set up websites for their corporate businesses, which are different portals from websites that consumers use. For example, Walmart has a corporate website (https://corporate.walmart.com/) aside from the online retailing website (https://www.walmart.com/) that consumers are familiar with. We coded both consumer websites and corporate websites to examine the consistency of compliance in the companies. Some of the companies in the list are holding companies which hold various brands underneath. For those holding companies, we randomly selected three brands under the holding companies and performed the categorization manually due to that the categorization scheme provided by Fortune 500 cannot be applied to those. In sum, a total of 125 websites are examined for the analysis.

Coding Procedure

A coding scheme was developed to examine the operationalization of GDPR compliance. For each website, we coded the presence or absence of the privacy banner. How websites obtain consent from their users and the information presented on the privacy banners are documented. These coding procedures determine whether websites are following the principle of lawful mandated by GDPR. Further, we coded the amount of information presented in the full report of privacy policy in the websites based on GDPR in examining whether the principle of transparency is met.

Results

One hundred and twenty-five websites are examined and we found that companies differ in how they comply with GDPR. In the first part, we examined the compliances and analyzed the patterns of strategies used by the companies. In the second part, we investigated the experiences of browsing these websites from perspectives of web visitors based on different regions.

Consent

Across all the websites examined, only 36 of them obtain consent from users, which means less than 30% of our selected websites are obtaining users consent as the legal basis for collecting and processing personal data. Of those websites that are obtaining consent through privacy banners, different patterns of strategies emerge. We categorized them into three types of privacy banners based on their interaction options: soft opt-in, implied consent, and explicit consent.

Soft Opt-in

Soft opt-in is the most frequently used strategy for privacy banners. Among all the websites, 27 websites use the strategy in obtaining their consent as their legal basis for data processing. The type of privacy banner serves only for informational purpose. It informs users of the data collection and indicates users that by continue browsing the website, they are consenting to the use of cookies. Despite that a button for "accepting" or "agreeing" the term is placed on the banner, there's no mention of how users can opt out of such data collection, leaving users no choices

but to accept it if they wish to use the services. Some websites even include a button "X" for closing the banner, but closing the banner does not suggest the declination of data collection. Cookies are used even if they actively click the closing button.

An example of this would be the website of Samsung. It presents a pop-up privacy banner at the bottom of the page with the text "This site uses cookies to enhance your website experience. By continuing to browse or use this site, you are agreeing to our use of cookies. See our privacy policy here." A link to the full privacy policy is attached, and an "X" for closing the banner. Therefore, by continuing to use the site, users will automatically be agreeing to the use of cookies even if they click the close button.

Implied Consent

One level above soft opt-in is the strategy of obtaining users' implied consent. Websites present privacy banners informing users that cookies are already in use, but users can opt out of cookie placements by following the instructions. This strategy, along with soft opt-in, is questionable because GDPR stipulates that silence, pre-ticked boxes and inactive are not considered a valid consent.

An example falls under this category is the website of Dell Technologies. On the website of Dell Technologies, an orange box "cookie consent" is located at the left bottom of the page. When clicked, descriptions of the use of cookies and purposes of each cookie are presented. Visitors can opt-out of cookie that they do not wish to place in their computers. However, without actively clicking the box, visitors will never be informed of the use of cookies.

Explicit Consent

The only strategy emerges from our analysis that meets the requirement of GDPR is explicit consent. With explicit consent, a clear affirmative action is performed by the users. Data are collected after users have clicked the button of "Agree" or "Accept". Remaining silence or inactive when browsing the site will not result in the use of cookies. Users are presented with options of not giving consent without degraded versions of the services. At the same time, withdrawing consent is as easy as giving it.

The website of Air France, for instance, obtains users' explicit consent for data collection. When landing the page, users are prompted with a privacy banner suggesting that the website use cookies for enabling proper functions and security as well as offering users the best possible user experience. Users can either choose to click on "Agree" or change the cookie settings on the banner. It is also specified that changing the setting of cookie is possible at any time. On the banner, cookies are categorized into functional cookies, analytical cookies, and marketing cookies. Users can opt out of the use of analytical and marketing cookies.

Levels of Compliance

According to GDPR, only by obtaining explicit consent can be considered compliance to the regulation. We consider those that obtain implied consent and those that use soft opt-in as partial compliance. By examining how websites obtain consent and information provided in the privacy policy, we categorized websites into three levels of compliance, full compliance, partial compliance, and non-compliance based on the analysis.

Full Compliance

Websites that are fully complied with GDPR strictly followed GDPR's three principles: lawful, transparency, and fairness. The principle of lawful is manifested by obtaining visitors explicit consents for processing data through a non-disruptive measure. Apart from that, the identity of data controllers, the types of processed data, as well as the purpose of the processing are clear to the

visitors in compliance with the transparency principle.

An example that qualified as a fully GDPR-complied website is the website of Lufthansa Airline. When visitors land on the page for the first time, they are informed of the use of cookies to ensure high-quality standards by a pop-up banner appear on the bottom of the website. The purposes of using cookie are described as "functional, statistical and comfort reasons as well as displaying personalized content." Visitors can give consents for processing data by clicking "Yes, I agree" or change the cookie settings easily by clicking the button presented on the banner.

If users clicked the button for changing their cookie setting, a panel with cookie descriptions will be called up. Four types of cookies are listed, including necessary, statistic, comfort, and personalization. A short description is provided under each type of cookie. Except for the "necessary" type of cookies, visitors can choose to opt out any type of the other three types. Once the panel is closed, the cookie changing panel can be called back by scrolling down the webpage and click the "Change Privacy Setting" button. This indicates that visitors have the right to withdraw consent anytime. The privacy policy of the website is found under the label of "Data Protection." The controller of the data and the contact information of a data protection officer are listed on the top of the privacy policy. The purpose of processing data is listed in detail, specifying that each purpose is based on different legal bases with specific GDPR articles. It is also mentioned that consent given by the visitors can be withdrawn at any time. Retention period of visitor data and the recipients of the data are listed in the policy. As for the recipients of visitor data, various agents are mentioned to be receiving the collected data, including service providers related to "the provision of the website, newsletter dispatch, feedback handling, creation of international aviation statistics." No specific company or third-party are named. Visitors' rights are listed in bullet points with specific GDPR articles. The section is followed by instructions on how visitors can exercise these rights. The rights to withdraw consent is stress again. The use of third-party cookies and purpose for each are then explained below.

Partial Compliance

Some of the websites are considered partially complied with GDPR. These websites fail to comply various aspects of the consent and transparency principles. Without obtaining explicit consent, they adopt soft opt-in or obtain implied consent for processing personal data. For some, they failed to meet the requirements of providing enough information that GDPR requires.

Transparent information should be provided when users are requested for consent and in privacy policy which users have full access to. According to GDPR, visitors should be notified of the controller's identity, the data being processed, the purpose of processing and the right to withdraw consent. Purpose of processing should be stated, and separated consent should be given if the processing is served for multiple purposes. However, some websites do not present information clearly to visitors when obtaining consent; instead, short, vague purposes are provided when requesting consent from visitors.

The website of Circle K explains the purpose of data collection with a short sentence of "ensure the best experience." Similarly, the website of Ceconomy describes the use of cookies as providing "a pleasant online experience." The website of British Airway does not indicate any purposes at all. These websites do not provide a solid purpose of cookie use, nor do they obtain separate consent for multiple purposes. There is no mention of users' rights of withdrawing consent, either.

The lack of transparency in the privacy policy is also found in our analysis. According to the regulation, visitors should have

transparent access to the rights, including the rights to access their data, rights to rectify their data, etc. Moreover, the language describing them should be easy and plain. However, websites have been found to cramp all rights together, results in difficulties in reading and understanding the rights.

An example of this is the website of Watsons. In the privacy policy found on the website, there is no mention of rights regarding how visitors can delete their data. Same as Watsons, the privacy policy found on the website of Homesense only present the rights to access, update and correction of inaccuracies, lacking any instructions of how visitors can delete any personal data. In fact, the right of forgotten, the right to restriction of processing, and the right to data portability are the least described rights among other rights posed by GDPR.

Some websites only acknowledge the rights of those who have created accounts on the website with no instructions on how non-member of the website can access, rectify or delete any information held by the website. The website of Kroger is an illustration of this. The privacy policy indicates that visitors with an account can manage subscriptions to email, mobile and online communications programs through its preference settings. However, there is no mention of how people without an account could access or delete their information. Some websites follow GDPR on a more loose level, with no user rights presented at all. Such as the website of JD.com, while visitors have access to a privacy policy, information of visitor rights are not provided on the page.

Non-compliance

For non-compliance websites, there is no indication of the collection and processing of visitor information. The principles of lawful and transparency are not met. The most common pattern appears in the category is the lack of obtaining consent before processing user data. These websites are using cookies, but they do not inform their users thereof. Only when users access the privacy policy or click around certain pages will they find related information.

Walmart, for example, uses cookie son its website but does not inform their visitor when they land on the page. The use of cookies is not stated in the privacy report, and users can only gain related information in the "Frequently Asked Question" section. Another example of this is the website of China post. The website is indeed placing cookies on visitors' computers, but there is no information regarding the collection and processing of user data, neither a full privacy policy.

Other Patterns

Besides patterns described above, a few trends of compliance strategies have emerged in our analysis. First, while most privacy banners are placed either on the top or bottom of the landing page, some businesses place their privacy banners in the middle of the page, blocking the view and that users are forced to make decisions, either giving consent to data collection or adjusting their cookie preferences before they can use the services.

Second, the compliance of the company website under the same parent company is not necessarily consistent with each other. For instance, websites designed for consumers and websites designed for corporate informational usage do not always reflect the same strategy, either. The website of Air France-KLM's holding company contains a banner informing users that cookies will be used if they continue to use the website without giving options of opting out the data collection. This is different from what is presented in the consumer portal websites of both Air France and KLM. Both websites obtain users explicit consent before processing personal data with a cookie-setting changing panel attached for users to opt out of any cookies. However, the two websites differ in their languages describing the cookie usage.

The website of KLM describes more details in the different purposes of functional cookies, analytics, and marketing cookies. The purpose of using third parties are also explained. On the other hand, the website of Air France provides a much more concise description of the purpose of using cookies, with no mentions of any third parties.

Vertically, the compliance between parent companies and subsidiaries are not always consistent with each other, either. For some corporates, privacy banners are presented for obtaining consents, but the same information is not presented on consumer websites of individual brands. Honeywell's corporate website obtain visitors consent through a privacy banner; however, Honeywell's website for its regional stores, which is the website of consumer portal, does not have any indication of informing visitors of the collecting and processing of the data.

On the contrary, there are corporates that illustrate the opposite strategy, presenting privacy banners for obtaining consent only on consumer websites but not on corporate websites. Websites of Lufthansa's consumer website obtain users explicit consent through a banner. However, the group's website of Lufthansa, where corporate news and information of investor relations are provided, does not provide visitors cookie opt-out choices for visitors who visit the website.

Global Strategy

We delved into how visitors differ their experiences when visiting these websites based on different regions. GDPR are regulations designed to protect the privacy and data of EU citizen. Therefore, companies across the globe have adopted different strategies for collecting data from EU users, and different levels of compliances emerged. While websites based in EU are almost consistent in how they comply with GDPR facing visitors across the globe, websites based out of EU differ in how they comply.

Three patterns of compliance strategy emerged for non-EU websites when dealing with EU users. They either comply with GDPR within a global context, comply only for EU users, or block EU users from using the services.

First, some websites have adopted the same strategy in obtaining users consent regardless of their regions. For example, the website of Samsung presents a cookie banner and inform their users of the use of cookies regardless of users' IP address.

Second, some websites distinguish EU users from other regions and follow the rules of GDPR only when facing them. Among these websites, strategies differ in how they identify EU users. The more common one is to identify users using their IP address. Example of this would be the websites of IBM. When visitors enter the website of IBM using a German IP address, the website presents a privacy banner indicating that cookies are used on the site. Specific purposes of using cookies are provided. The banner also informs visitors that cookie preferences will be shared with other IBM web domains, with specific domains listed. The banner also allows users to change their cookie preferences if they do not wish to have the cookies placed. This is different from using a US IP address and a Singapore IP address through which no notification is provided to the users of the use of cookies, nor does the site obtain consents from visitors or give visitors any choices in opting-out any of the cookies.

On the other hand, it has been found that even if a user is not geographically located in EU regions but shows an EU preference, for example, set the preferred language to European language, or the region setting to countries of EU, some websites will consider the visitors as EU citizen. United Airline identifies users as an EU citizen when the region setting on the webpage is selected as Germany. When visitors change their region setting to Germany, a privacy banner appear at

the top of the page informing visitors that cookies are used. However, the banner disappears automatically after a few seconds without visitors giving consent. Meanwhile, when users enter the site from a German IP address with US-English region setting, the website does not identify the visitors as EU visitors and therefore does not present any privacy banner informing them the use of cookies.

Third, some websites have been found that they completely block out EU visitors from entering. Examples of blocking EU visitors are websites of T.J.Maxx and Home Depot. When entering the website of T.J.Maxx with a German IP address, a blank page shows up with the message saying "We're sorry, tjmaxx.com is unavailable in your country." Similar to this, the website of Home Depot is completely inaccessible to visitors with German IP address.

Discussion

The findings derived from the case studies illustrate that companies differ in their compliances of GDPR. We found that consent is not obtained in the majority of the examined websites and consumers are not informed of the data collection. In addition, for those businesses that do notify their users of data collection, various strategies are discovered and not all adoptions of privacy banner meet the requirements.

Managerial Implications

From an industry point of view, we recommend businesses re-examine their privacy policies and investigate whether their compliances meet the requirements of GDPR. Instead of providing information to consumers, privacy policies are often made to protect businesses against lawsuits, overflowed with legal jargons (Pollach, 2005). Studies have shown that privacy notices can be a trust-building communication bridge for businesses and decrease the risk perception of sharing personal data if the messages conveyed are informative (Milne and Boza, 1999; Culnan and Milberg, 1998). It can also build a positive reputation with consumers (Schonenbachler and Gordon, 2002). Henceforth, it is recommended that businesses should treat their privacy policies as a bridge for communication with consumers, rather than mere legal documents. In terms of both privacy banners and privacy policy, we provide three suggestions for businesses: be clear, be straightforward, and be relevant.

Be clear on how data is used and who will be shared with. Studies have shown that lacking information with regards to how personal data is used can lead to refusal in providing personal data (Luzak, 2014). With clear information provided, for example, a privacy banner, consumers can make their decisions on information disclosure more easily.

Be straightforward in the languages used in privacy policies. It has been suggested that consumers don't read privacy notices because they are long and hard to understand (Milne and Culnan, 2004; Luzak, 2014). Messages conveyed in a straightforward style can result in more trust and encourage consumers to read them (Milne & Culnan, 2004; Schoenbachler and Gordon, 2002).

Be relevant in content. Consumers are more likely to read the messages if the content seems personally relevant (Milne and Culnan 2004). Luzak (2014) also suggests that privacy notices should be attractive to consumers. Privacy policies should not only draw consumers' attention but encourage consumers to read it.

Limitations and Future Works

The project seeks to shed some light on GDPR compliances by examining websites of various sectors relevant to consumers. We focused on how businesses convey messages to consumers and how they obtain consents. Futures studies can further investigate

consumer attitudes and behaviors toward various levels of GDPR compliance. For example, consumers' willingness or reluctance on sharing cookies with businesses or third-parties can be discussed. A number of factors have been identified in previous research that leads to the reluctance in self-disclosure online, including trust (Milne & Culnan, 2004; Poddar, Mosteller, & Ellen, 2009; Metzger, 2006), website reputation (Xie, Tao, &Wan, 2006), risk (Miyazaki & Fernandez, 2001), emotion (Li, Sarathy, & Xu, 2010; Wakefield, 2013), and motivation (Poddar et al., 2009).

Related to the topic of information disclosure, scholars have proposed that people perform a cost-benefit analysis for making decisions on sharing personal data, which is termed "privacy calculus" (Laufer & Wolfe, 1977). More specifically, individuals are more likely to disclose personal data if the benefit outweighs the cost of not disclosing it. In the context of data collection and consent requests from businesses, consumers may analyze the benefits and consequences of giving consent when browsing websites (Culnan & Bies, 2003; Phelps et al., 2000). If rewards are provided, consumers are more likely to provide personal information (Xie et al., 2006). In light of this, future studies can delve further into how message framing on the privacy banner affect the exchange of personal data between consumers and businesses.

Conclusion

The project aims to examine the compliance of GDPR among websites in hopes of having a clearer idea on whether businesses of various sectors are meeting the requirements of the regulations. While the industry of digital advertising grows evidently, not all businesses are complying with GDPR consistently and provide consumers with transparent information. However, with frequent outbreaks of data breaches, both consumers and businesses are undoubtedly affected by how they value personal data. In 2018, more than three thousand publicly disclosed global data breaches have been reported and 3.6 billion records have been exposed (Ausick, 2018). The issues of data protection should be taken seriously. While we only investigate businesses from a GDPR framework, regions besides EU have also been introducing regulations designed to protect consumer data. For example, the US has passed the California Consumer Privacy Act (CCPA), which will go into effect in 2020, goes beyond notification on data breaches and require businesses to make changes to their data processes. In recent years, Asia-Pacific countries have also tightened their data protection environment, with Australia and Japan amended their privacy law in 2017 (Hasan, 2018). The topics of data protection and privacy on the internet are not expected to be waning soon. In sum, it's inevitable that GDPR will bring changes to operations of businesses. Businesses should be fully prepared with regards to the privacy issue and create a friendly environment regarding data protection for consumers.

References

Glass, R., & Callahan, S. (2015). *The big data-driven business how to use big data to win customers, beat competitors, and boost profits*. Hoboken, NJ: Wiley.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2018). We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. Retrieved November 14, 2018, from the arXiv database.

TrustArc. (2017). *Privacy and the EU GDPR: US and UK privacy professionals.* Retrieved November 14, 2018, from https://www.corporatecomplianceinsights.com/wp-content/uploads/2017/11/TrustArc-Privacy-and-the-EU-GDPR-Research-Report-09.26.17.pdf

Ponemon Institute. (2018). *The race to*

GDPR: A study of companies in the United States & Europe. Retrieved November 14, 2018, from https://iapp.org/resources/article/the-race-to-gdpr-a-study-of-companies-in-the-united-states-europe/

Cybersecurity Insiders. (2018). *GDPR compliance report.* Retrieved November 14, 2018, from https://crowdresearchpartners.com/wp-content/uploads/2018-GDPR-Compliance-Report.pdf

PwC. (2018). *IAB internet advertising revenue report 2017 full year results.* Retrieved November 14, 2018, from https://www.iab.com/wp-content/uploads/2018/05/IAB-2017-Full-Year-Internet-Advertising-Revenue-Report.REV2_.pdf

McNair, C. (2018, October 16). *US ad spending 2018 - eMarketer trends, forecasts & statistics.* Retrieved from https://www.emarketer.com/content/us-ad-spending-2018

Libert, T., Graves, L., & Nielsen, R. (2018). *Changes in third-party content on European news websites after GDPR. Reuters Institute.* Retrieved from https://reutersinstitute.politics.ox.ac.uk/our-research/changes-third-party-content-european-news-websites-after-gdpr

Schiffner, S., Berendt, B., Siil, T., Degeling, M., Riemann, R., Schaub, F., ... & Polonetsky, J. (2018). Towards a roadmap for privacy technologies and the general data protection regulation: A transatlantic initiative. In *proceedings of the Annual Privacy Forum 2018*.

Kulyk, O., Hilt, A., Gerber, N., & Volkamer, M. (2018). "This website uses cookies": Users' perceptions and reactions to the cookie disclaimer. *European Workshop on Usable Security (EuroUSEC) 2018*. Retrieved from https://dx.doi.org/10.14722/eurousec.2018.23012

Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 1-20.

Pollach, I. (2005). A typology of communicative strategies in online privacy policies: Ethics, power and informed consent. *Journal of Business Ethics, 62*, 221-235.

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity.* 1-20.

Tjong Tjin Tai, E. (2016). The right to be forgotten–private law enforcement. *International Review of Law, Computers & Technology, 30*, 76-83.

Malle, B., Kieseberg, P., Weippl, E., & Holzinger, A. (2016, August). The right to be forgotten: towards machine learning on perturbed knowledge bases. In *International Conference on Availability, Reliability, and Security* (pp. 251-266). Springer, Cham.

Milne, G. R., & Boza, M. E. (1999). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing, 13*, 5-24.

Culnan, M. J., & Milberg, S. (1998). The second exchange: Managing customer information in marketing relationships.

Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing*, *16*, 2-16.

Luzak, J. A. (2014). Privacy notice for dummies? Towards European guidelines on how to give "clear and comprehensive information" on the cookies' use in order to protect the internet ssers' right to online privacy. *Journal of Consumer*

Policy, 37, 547-559.
Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*, 15-29.
Poddar, A., Mosteller, J., & Ellen, P. S. (2009). Consumers' rules of engagement in online information exchanges. *Journal of Consumer Affairs, 43*, 419-448. doi: 10.1111/j.1745-6606.2009.01147.x
Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research, 33*, 155–179. doi: 10.1177/0093650206287076
Xie, E., Teo, H. H., & Wan, W. (2006). Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. *Marketing Letters, 17*, 61-74. doi: 10.1007/s11002-006-4147-1
Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs, 35*, 27-44. doi: 10.1111/j.1745-6606.2001.tb00101.x
Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems, 51*, 434-445. doi: 10.1016/j.dss.2011.01.017
Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems, 22*, 157-174. doi: 10.1016/j.jsis.2013.01.003
Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. Journal of Social Issues, 33, 22-42.
Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. Journal of Social Issues, 59, 323-342.
Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*, 27-41. doi: 10.1509/jppm.19.1.27.16941
Hasan, N. (2018, February 1). Data Privacy Law in the Asia-Pacific Region. Retrieved from https://staysafeonline.org/blog/data-privacy-law-asia-pacific-region/
Ausick, P. (2018, November 08). Data Breaches Have Exposed 3.6 Billion Records So Far in 2018. Retrieved from https://247wallst.com/technology-3/2018/11/08/data-breaches-have-exposed-3-6-billion-records-so-far-in-2018/
Moses, L. (2018, July 02). US sites continue to block European visitors post-GDPR. Digiday. Retrieved from https://digiday.com/media/u-s-sites-continue-block-european-visitors-post-gdpr/