The Convention on Monitoring Advertisers and Limiting their Targeting Endeavors

(The MALTE Convention)

Rebecca Zuo and Hyun Choi

11 December 2020

CSCI 2390, Brown University

Introduction

Threats of targeted advertising and overly loose guidelines could include technology redlining based on income or race, influencing voting outcomes, or even government surveillance. In addition, consumer trust in a company also impacts customer acquisition and retention. For instance, The Harris Poll found out that 75% of people that don't trust a company with their data wouldn't buy from that company, no matter how great its products and services (Villi). While the introduction of the General Data Protection Regulation (GDPR) in the European Union has largely been a positive force for consumer data privacy in the modern era, there are still large issues with its implementation in the field of targeted advertising that must be addressed. So far, techniques used for tailoring targeted advertising such as the use of cookies and third party tracking, which is allowed as long as there is explicit user consent, and that the tracking is being done for a legitimate cause. However, a lot of ambiguities emerge with what is considered explicit consent, and with whether or not advertising should be considered legitimate interest. In large, we must balance realistic business interest with protecting user privacy while considering that guidelines are not absolute, should be considered in relation to its function in society, and should be balanced against other fundamental rights such as freedom of expression. In this paper, we aim to explore the issues currently plaguing the GDPR due to its ambiguities, examine legislation currently enacted and pending in both South Korea and the United States, analyze the feasibility of a technical and mathematical approach to data privacy legislation, and ultimately propose a new international treaty that would create one unified data protection and targeted advertising regulation scheme to benefit consumers and businesses alike.

SECTION 1: PROBLEMS WITH THE GDPR

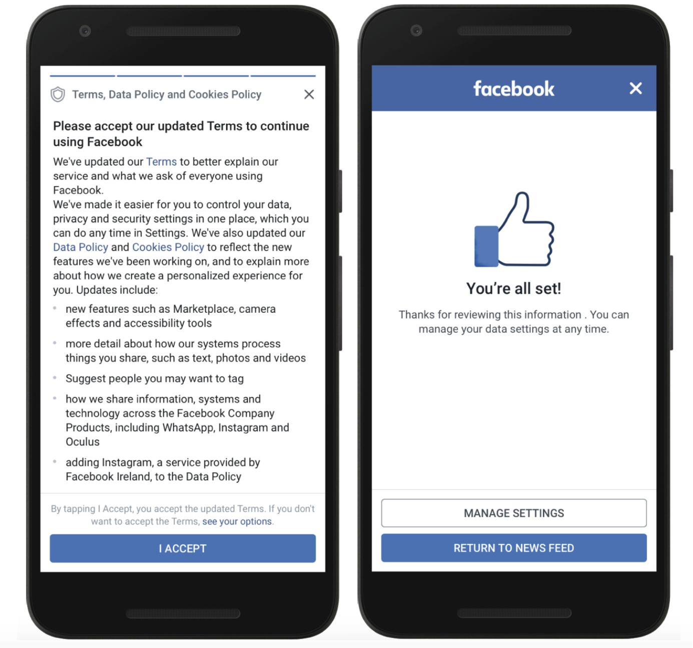
1.1. User Consent

Ad Personalization depends heavily on programmatic behavioral targeting, there are several things that personal identifying information (PPI) could entail. For instance, social security number, IP address, coordinates, mobile identifiers, biometric, financial, behavioral, demographic data are all things that advertisers can use to build an user profile and would fall under the category of PPI under the GDPR. Under the GDPR, such personal identifying information requires user consent to be used by a company.

User consent is stated explicitly in article 4 of the GDPR:

Article 4: 'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

What isn't specified explicitly is what level of information companies would have to provide for the user, in order for consent to be explicit . For instance, in what detail does information need to be provided on how the information is being processed and used by third party advertisers. Would stating, "we are using your IP address , mobile information, and browsing behavior to create more targeted advertisements" sufficient? Or does the usage of every piece of data need to be outlined. For example, stating "the IP address is being used to target local-level products, and Mobile information collected is being used to monitor in-app behavior." The GDPR takes an opt-in approach while the California Consumer Privacy Act (CCPA) takes an Opt-in approach. Hence, the implementation of these guidelines vary based on particular use cases, and could be as nuanced as user interface design. This raises the question, how can we create new guidelines that would make design requirements for consent to be more explicit?



Terms, Data Policy and Cookies Policy

Please accept our updated Terms to continue using Facebook

We've updated our Terms to better explain our service and what we ask of everyone using Facebook.
We've made it easier for you to control your data, privacy and security settings in one place, which you can do any time in Settings. We've also updated our Data Policy and Cookies Policy to reflect the new features we've been working on, and to explain more about how we create a personalized experience for you. Updates include:

- new features such as Marketplace, camera effects and accessibility tools
- more detail about how our systems process things you share, such as text, photos and videos
- Suggest people you may want to tag
- how we share information, systems and technology across the Facebook Company Products, including WhatsApp, Instagram and Oculus
- adding Instagram, a service provided by Facebook Ireland, to the Data Policy

By tapping I Accept, you accept the updated Terms. If you don't want to accept the Terms, see your options.

You're all set!

Thanks for reviewing this information . You can manage your data settings at any time.

Here we see the consent forms for Facebook, which technically has an opt-out in the small "see your options" link. This feature is obscured by the large "I accept" button.

Under the CCPA, users must have a clear and conspicuous link on their website titled "Do Not Sell My Personal Information" that gives consumers the option to opt out of the sale of their personal information. Businesses must then wait 12 months again before asking to sell data. Selling data entails the "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration." There could be some ambiguity here for advertisers regarding what is considered a sale. In terms of third-party cookies for targeted or behavioral advertising, giving a third party network access to consumer information could be considered "a sale" under the CCPA(Focalpoint). To prevent cookies being considered sales, for advertisers to adhere to CCPA compliance, they often will also use cookie banners to signify that the user has intentionally disclose personal information.

Furthermore, what is considered personal data could also vary based on context. For instance, the CCPA defines personal data as “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.” What should be considered personal information is also a point of contingency. For instance, in California, IP addresses aren’t considered personal information if they are not linkable to a specific person or household. The New York Shield Act also has different specifications for personal identifying information to include account username and password. The inconsistencies across different privacy legislations raises the question, what should we limit the scope of personal data to in terms of advertising?

1.2. Granularity

The GDPR also requires granularity. As defined below:

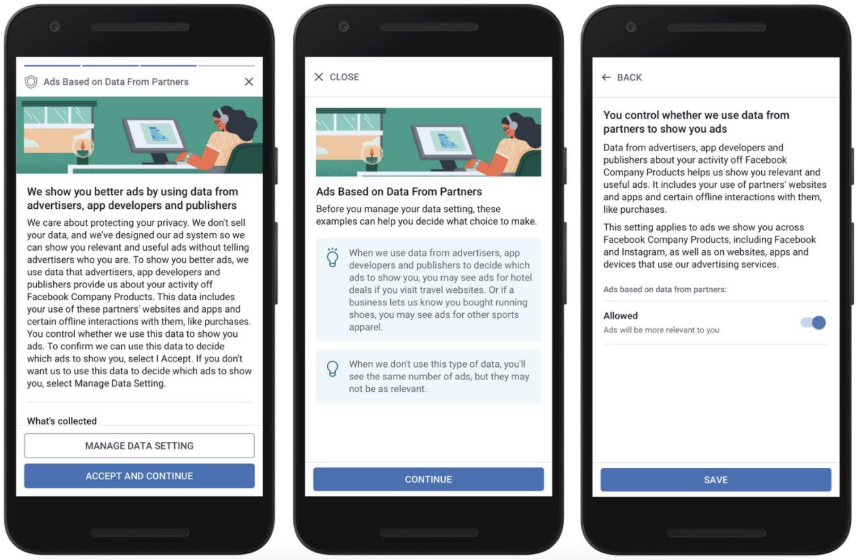
> *3.1.3 Granularity*
>
> *42. A service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes. In a given case, several consents may be warranted to start offering a service, pursuant to the GDPR.*

In the case of targeted advertising, granularity implies that in terms of tracking web behavior , there needs to be a way for granting access to control over cookies and trackers under the idea that the user owns the data. For instance, “cookie walls,” which allow the user to either take it or leave it by accepting all cookies before they access content are technically not compliant (UK

Information Commissioner's Office). With the strictest interpretation, granularity would involve individual opt-in check boxes for each individual cookie, and the specific controllers or processors involved with that data collection. Some of the potential parties involved could include the ad server, the exchange (which enables advertisers and publishers to buy and sell in the advertising space), Data Management Platforms (DMP), and the Digital Signal Processor (DSP). Under the GDPR, any of these parties could be liable if there was an illegal use of data.

However, this remains an ambiguity in the GDPR, and few companies currently exercise this. For instance, cookie sharing often takes place between the DMP and DSP to increase the level of cross-site tracking and targeting that cookies provide in a process called cookie syncing that takes place in the form of cookie banners. Usually, when a DSP creates a third party cookie, other vendor cookies are dropped for matching. The DMP can also create its own third-party cookie that can be dropped. The DMP and DSP can now communicate between the cookies (Shuptrine). This usually happens before user consent, or even if consent is given, most of the time the user won't look at the fine text of what types of cookies are being used. Similarly, the CCPA also allows the website to fire cookies before the website user accepts them as long as you give them the information about data you're collecting at the point of collection (Red Clover Advisors). Certain types of cookies could be considered exempt if they are essential to the function of the website such as those used for "User Input" or "Authentication." These same rules apply to the CCPA and New York Shield Act. However, non-essential cookies require explicit consent. Ultimately, pre-determining non-essential cookies provides a nudge like behavior for the user to accept the cookies. This is an area that could use stricter protocols for ensuring that the user consent is actually explicit and uninfluenced.

Under the CCPA there is also the additional requirement to delete their personal data from the business's storage with the “Do not sell” link for opt-out requests. This is a more globalized opt-out that differs from the GDPR’s granular approach. The CCPA proposes a model such that businesses must respect a “global privacy control” sent by a browser or device. This would essentially remove the possibility of all targeted advertising, by letting the user set settings once through a server or browser extension such as Chrome's “do not track setting” (Edelmen). The user could then opt-in or grant exceptions to particular companies. Some ad-companies have considered these regulations as an unconstitutional limitation on free speech. Even though past precedents with telemarketers and “do not call” did not succeed with similar claims, such regulation could be too extreme on businesses that rely predominantly on ads for revenue (Shultz). The GDPR provides no right for users to opt-out of personal data sales, but it does provide consumers the right to opt-out of processing data for marketing purposes, and withdraw consent to process personal data. A question that arises is how granular should consent be, while still balancing the fundamental right to conduct business?



We show you better ads by using data from advertisers, app developers and publishers

We care about protecting your privacy. We don't sell your data, and we've designed our ad system so we can show you relevant and useful ads without telling advertisers who you are. To show you better ads, we use data that advertisers, app developers and publishers provide us about your activity off Facebook Company Products. This data includes your use of these partners' websites and apps and certain offline interactions with them, like purchases. You control whether we use this data to show you ads. To confirm we can use this data to decide which ads to show you, select I Accept. If you don't want us to use this data to decide which ads to show you, select Manage Data Setting.

What's collected

Ads Based on Data From Partners

Before you manage your data setting, these examples can help you decide what choice to make.

When we use data from advertisers, app developers and publishers to decide which ads to show you, you may see ads for hotel deals if you visit travel websites. Or if a business lets us know you bought running shoes, you may see ads for other sports apparel.

When we don't use this type of data, you'll see the same number of ads, but they may not be as relevant.

You control whether we use data from partners to show you ads

Data from advertisers, app developers and publishers about your activity off Facebook Company Products helps us show you relevant and useful ads. It includes your use of partners' websites and apps and certain offline interactions with them, like purchases.

This setting applies to ads we show you across Facebook Company Products, including Facebook and Instagram, as well as on websites, apps and devices that use our advertising services.

Ads based on data from partners:

Allowed ●
Ads will be more relevant to you

Photo: TechCrunch

For example, as seen above, in order to be GDPR compliant Facebook allows the user to block ads based on browsing behavior on websites that show likes, shares, conversion pixel, or audience network ads. However, according to TechCrunch, there are no restrictions on how Facebook is using the data to personalize the News Feed or for other parts of its service (Constine). It also provides no specification of what partnering websites constitute, and how the data could be used beyond the scope of Facebook's services. Additionally, the Ad Preferences menu is hard to find and difficult for the average user to use. The menu does allow users to opt-out of certain ads such as for alcohol, or for children, but doesn't specify the types of information collected to result in such targeted advertisements (Costine).

1.3. Turning Towards First Party Data

As a result of the nuanced consent regulations presented by the GDPR or CCPA, companies have turned towards first party data collection and first party cookies. This can ensure that the company and user has a clearer understanding of how the data is being collected, processed and for what purpose. First party data collection improves the user's trust, by minimizing "creepy advertising," and users not understanding why they are being shown certain ads. First party data most likely won't be shared with other companies. At the same time, companies can still use first party data to target ads within the platform using the following four approaches: Personalization, Segmentation, Lookalike marketing, and Using analytics and AI (Shuptrine). For instance, an user's specific demographic data could be tied to behavioral data such as "shoe lover," which can be tied to a unique hash id or cookie id. Then these users can be grouped and segmented and provided particular ads. It is easier for companies to argue that they have a legitimate interest in using these approaches when only first party data is involved.

1.4. GDPR Article 6(1)(f) — The "Legitimate Interests" Basis

In contrast to asking for explicit consent to process a user's data, the Article 6(1)(f) of the GDPR allows for data processing in the case that:

> processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

The text of the Regulation is silent on what exactly constitutes a "legitimate interest" on the part of the data controller, but the European Court of Justice has confirmed a three-part test approach for evaluating a controller's legitimate interest (EUR-Lex). This three-part test is broken down into the Purpose Test, the Necessity Test, and the Balancing Test. UK regulators suggest that anyone intending to process user data using the legitimate interests basis should conduct a "legitimate interests assessment" evaluating each one of the three tests to determine whether their data processing is justified under the GDPR (UK Information Commissioner's Office).

The first two tests are fairly straightforward and relatively easy to meet, or at least, create a plausible justification. The Purpose Test asks whether there is a "legitimate interest" behind processing the data. This interest does not have to be "very compelling," and it could even be a relatively trivial purpose. As long as the controller has a "clear and specific benefit or outcome in mind," the Purpose Test is met. The Necessity Test states that the controller must demonstrate that the data processing is necessary to achieve the legitimate interest identified in the Purpose Test. The data processing has to be done in the least invasive way possible, and if there is "another reasonable and less invasive way to meet the interest and achieve your purpose without the processing," then that approach must be taken.

The final test, the Balancing Test, is most relevant to our normative analysis of data processing and the GDPR. The controller must evaluate whether that legitimate interest is outweighed by the "individual's interests, rights, or freedoms," and if it is, data processing must not occur. The standard used with this test is whether a reasonable person would expect the processing of personal data in a particular situation. Notably, this test disregards what the actual individual users in question expect in data processing, but rather "objectively" looks at what a "reasonable person" should expect. Ironically, this test that regulators frame as an "objective test" makes it even more difficult to ascertain whether the processing of data is appropriate in a given situation. The expectations of a "reasonable person" will differ wildly depending on their background, technical knowledge, and previous experience with the matter. The UK regulators even admit there is "no exhaustive list" of factors to consider when considering the balancing test, but at a minimum, the following should be considered:

- The nature of the personal data to be processed,
- The reasonable expectations of the individual, and
- The likely impact of the processing on the individual and whether any safeguards can be put in place to mitigate negative impacts.

Of course, it is impossible to codify every permissible and impermissible situation in which data may or may not be processed. The "reasonable person" standard is actually used in many legal statutes where it is difficult to lay out every single situation that may apply to a given law. But the current scheme of conducting the Balancing Test is overly vague and must be reformed such that data subjects can be confident in how their data is being used and companies have clearer guidelines under which to conduct operations.

1.5. GDPR Article 22(1) — Automated Individual Decision Making

Article 22 of the GDPR addresses and prohibits "automated individual decision-making, including profiling." This article has huge implications for targeted advertising, as most of the "targeting" is done in an entirely automated fashion. The text of Article 22(1) reads:

> The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

There are only three exceptions to this rule. As laid out in the very next subpart, automated individual-decision making is only permissible if it is (1) necessary as part of a contract between the data subject and the controller, (2) authorized by EU or member state law, or (3) based on the data subject's explicit consent. In general, companies that rely on targeted advertising seem to rely upon receiving explicit user consent when the user signs up for the service.

This article is particularly difficult to interpret in the context of targeted advertising, as it is difficult to comprehend what Article 22(1) specifically targets. If Google decides to serve an advertisement for Dell laptops because a user had searched for laptop reviews the day before, does that constitute a "decision" under the law, and if so, was that decision "based solely on automated processing," and further does this decision "significantly impact" the user?

The Article 29 Working Party, which advised stakeholders on the specific implementation of the GDPR until 2018, has interpreted "significantly impact" to mean that the "decision must have the potential to significantly influence the circumstances, behavior, or choices of the individuals concerned" (IAPP, Matheson). It is difficult to determine what would be considered a "significant influence." An example of a targeted advertisement that may be prohibited under this rule would be an ad for a gambling platform that was targeted to a user based on information that the user is part of a particular group that has higher rates of gambling addiction. It must be noted that the "legitimate interests" exception *does not* apply to Article 22, and so obtaining explicit user consent is the only way that a business may serve such targeted advertisements to a user (Sirius Legal). This is yet another

1.6. Case Studies on the Collection of Data for Advertising

On January 14 of 2020, the Norvegien Consumer Control filed a complaint against Grindr for potentially violating Article 9 of the GDPR. As soon as the user opens the app, advertisers received information for GPS location, device identifiers and the fact that one is using a gay dating app. Associating this information with an advertising ID then makes the user identifiable to third-party advertisers and across services. Beyond Grindr, other dating apps part of Match Group such as OkCupid and Tinder, could also be sharing data with each other regarding sexualities, drug use, and political views, according to *Bloomberg*(Porter). According to Article 9 of the GDPR,

> "the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited"

More particularly, the privacy policies for Grindr did not specify which third parties may receive personal data from the apps for advertising or analytics purposes. Below is their privacy policy outlined:

> *"We share your hashed Device ID, your device's advertising identifier, a portion of your Profile Information, Distance Information, and some of your demographic information with our advertising partners. These third parties may also collect information directly from you as described in this Privacy Policy through technology such as cookies. The privacy policy of these third party companies applies to their collection, use and disclosure of your information."*

What is to note is the vagueness of Grindr statement regarding the legal basis for processing data. By saying that "the privacy policy of these third party companies applies to their collection, use and disclosure of your information", Grindr is shifting accountability away from itself and to the advertising companies. It presents the use of tracking technologies as something beyond the scope of the application, making it difficult for users to understand what they are consenting to. According to the Norwegian Data Council, this is not GDPR compliant because Grindr is the data controller of personal data collected and shared through its services. Grindr only listed Twitter's MoPub as an advertising partner, and encourages users to read MoPub's privacy policies, but MoPub itself lists more than 160 partners(Forbrukerradet). This makes it nearly impossible for users to understand how their personal data is being used and for them to give explicit consent.

As a result of these accusations, Twitter dropped Grindr from their ad network over GDPR breaches but no official fines were made(Porter). However, what this case illustrates is the ambiguities in Article 4 regarding explicit consent and Granularity. In this case, Grindr did state that data was being used by third party advertisers but did not further explain, despite their role as the data controller. Stakes were even higher in this case due to the nature of the personal identifying data as outlined in Article 9, because data regarding sexual orientation was being collected. Ultimately, greater action should have been taken by data protection agencies to penalize and fine Grindr, in order to prevent future data sharing with third party groups with applications with special types of personal identifying data.

SECTION 2: DATA PROTECTION LEGISLATION FROM OTHER JURISDICTIONS

2.1. South Korea's Personal Information Protection Act

Now, let's examine the approaches of other jurisdictions to consumer data privacy. Most countries don't have such comprehensive laws, let alone laws specifically pertaining to targeted advertising, so we will examine data protection laws in general.

Following massive data breaches from Chinese hackers resulting in the theft of the personal information of the vast majority of the population, the South Korean government enacted the Personal Information Protection Act (PIPA) in 2011. This law instituted sweeping changes to how the country's tech sector stored and processed personal data. The PIPA defines "personal information" as "any information that can be used to identify a particular living individual" and specifically includes "information that can easily be used in aggregate with other pieces of information to identify an individual, even if any one particular piece of information cannot do so" (Korea Law Information Center and Korean Listed Companies Association, translated).

The Korea Communications Commission, recognizing the increasing prevalence of targeted advertising, published "Guidelines for Personal Information Protection in Online

Personalized Advertisements" in February 2017. Broadly, the Guidelines set forth four principles to which all "online personalized advertisers" must adhere:

(1) Transparency in the collection and usage of users' online activity,

(2) Guarantee of the users' right to control the usage of their data, including the right to opt out of providing data while still being able to use the service,

(3) Security of user data to prevent unauthorized usage or leaks, and

(4) Proactivity in informing the user of the company's targeted advertising practices, how such advertising functions, and the user's right to opt out of such advertising.

Initially, the PIPA was created to hold companies accountable for breaches of personal data such as Resident Registration Numbers (the equivalent of an American Social Security Number, but even more ubiquitously used) and "sensitive information" defined as "political beliefs, membership status in labor unions or political parties, medical and sexual information, and any other personal information that, if disclosed, has the potential to severely infringe upon the data subject's privacy" (Korea Law Information Center, translated). The law requires similar acts of explicit consent from the data subject like the GDPR, but where the PIPA differs from most other data privacy legislation out there is that violations of the law can result in criminal prosecution. It defines any "individual, corporation, government agency, group, etc. who processes personal information themselves or through a third party" as a "personal information processor." Any such processor who does not follow the law—for example, a website that does not receive explicit consent from the user when collecting data—can be fined up to $46,000 USD or be sentenced to a maximum of *five years in prison*.

At the same time, it is hard to see whether this law brought meaningful change in the data processing procedures of many Korean companies. Certainly, websites now have clearer and more prominent privacy policies for people to consent to, but the nominally harsh punishments laid out in the letter of the law do not seem to be enforced often. Prison sentences are handed down to individuals who happened to use personal information in the commission of other crimes, such as a student who hacked into their teacher's online accounts and harassed them who received 14 months in prison as a combined sentence for extortion and violation of the PIPA (South Korea Ministry of the Interior and Safety). Standalone PIPA violations where consent is not adequately obtained for information collection are not punished severely, often ending with fines on the order of $10,000 - 20,000 USD. In an unintended consequence, the PIPA has actually caused employees of many companies to avoid being in a situation where they must personally process personal information, as they are afraid they may be subject to criminal investigation if a breach occurs, while the company gets off relatively scot-free (ZDNet Korea).

Although the Korean system of punishment can be refined upon, we believe it is important to hold individual people who act as data controller accountable when the company breaks the law. In many cases, monetary fines simply become a cost of doing business if the potential profit of violating privacy outweighs the potential penalty. Personal liability simply creates an environment where compliance is valued due to the potential for personal consequences to an employee's own lifestyle, rather than just for the company's balance sheets.

2.2. Individual U.S. State Policies

Most notably the CCPA-compliance has an opt-out of personal data sales options, which allows consumers to opt-out, read, and delete their personal data from business storage. The CCPA also requires the disclosure of the financial incentives for selling or retaining personal consumer data. There is the potential possibility for a proposed "universal opt out" that wouldn't take place until 2023. With the global opt-out the idea is that instead of having to change privacy settings every time you visit a new site or use a new app, you could set your preference once, on your phone or in a browser extension, and be done with it (Edelman). This could potentially provide users with the opportunity to opt-out of any type of targeting advertising. For companies such as Facebook or Google Analytics that relies predominantly on advertising revenue, these measures could be too drastic. The current cookie requirements for the CCPA are similar to the cookie requirements of the GDPR and permit third party cookies if they are considered "essential" to the website or service. Another aspect of CCPA is that it only serves to regulate companies that have a gross revenue greater than $25M, handles personal data of more than 50,000 consumers for commercial purposes, or derives 50% or more of its annual revenues from selling consumers' personal data(CCPA). This differs from the GDPR, which regulates all businesses. Determining the scope of regulation could also be an important deterministic factor of balancing user privacy with business interests.

The New York Shield act expands what is considered private data to include an user's username and password, and biometric data such as voice prints(Baldwin). The scope of the shield act extends beyond New York and applies to any person or business that owns or licenses private information of a New York Resident. Similar to the CCPA, it has provisions that protect small businesses such as those with under 50 employees, or 3 million in gross annual revenue. It also creates an exception for instances such that "exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials." Here, the damages or threats of data mishandling were worded in terms of "financial harm" and "emotional harm", which are still ambiguous but provide greater specificity than the GDPR provisions of risks to the rights and freedoms of natural persons. Both the CCPA and the Shield act seem to address the financial value of data more directly than the GDPR.

2.3. Attempts at Federal Policy in the U.S.

On a federal level, data privacy in the United States is governed by a hodgepodge of various laws that govern the usage of data in specific contexts. For example, the Fair Credit Reporting Act (FCRA) governs the collection and processing of credit information, the Health Insurance Portability and Accountability Act (HIPAA) governs that of protected health information, and the Children's Online Privacy Protection Act (COPPA) governs the collection of data of children under 13 years of age (Congressional Research Service). However, there is no one overarching piece of legislation that governs data collection and processing of Americans that is comparable in level of protection that the GDPR provides Europeans. While the Federal Trade Commission does have the authority to regulate any companies engaging in "deceptive trade practices," this is not enough to fully regulate the tech landscape today.

In the couple of years since the enactment of the GDPR, there have been several attempts to enact federal legislation modeled after the GDPR and the CCPA. The Congressional Research Service's 2019 report on the subject advised that Congress must consider a wide variety of factors in creating data protection legislation, including codifying a well-designed definition of what information is to be protected, how a new law would interact with the existing laws such as HIPAA, and preemption of state laws (CRS). The last part is particularly important, as part of the advantages of a unified federal data protection law is that American companies would not have to spend time complying with different data protection standards in every single U.S. state and territory.

In late 2019, two bills were proposed in the U.S. Senate Committee on Commerce, Space, and Transportation to tackle this issue. A group of Democrats introduced the Consumer Online Privacy Rights Act (COPRA) while a group of Republicans introduced the Consumer Data Privacy Act (CDPA). These two bills share large portions that are similar in language, but sometimes diverge wildly. While neither bill advanced to a vote, the components in each of these bills give us an insight as to what laws may be palatable to modern day politicians.

Both bills require companies to obtain "affirmative express consent" before processing an individual's data, designate privacy officers within a company, and not deny goods or services to anybody who wishes to exercise a privacy right (Fazlioglu, IAPP). Privacy policies must be made "publicly and persistently available" in a "clear and conspicuous" or "conspicuous and readily available manner." Companies must conduct annual privacy risk/impact assessments under both laws, although the CDPA provides more details as to what is required from these assessments. Most notably for our study, both bills would require the Federal Trade Commission to "examine the use of algorithms to process data in ways that may violate federal anti-discrimination laws," while the CDPA goes further and would require the FTC to "develop guidance to assist covered entities in avoiding discriminatory use of algorithms." This process would almost certainly include an analysis of the current state of targeted advertising in the United States.

What is more interesting about these two bills, however, is how they differ. Particularly important to the goal of having one unified data protection regime in the United States is the notion that the federal law would preempt (or overrule) state law and in essence create one large jurisdiction for companies. The CDPA directly preempts any state law that is "related to the data privacy or security and associated activities of covered entities" (Fazlioglu, IAPP). Therefore, state laws such as the CCPA would cease to be enforceable on a state-by-state level, in favor of the one federal law that governs all relevant activities. On the other hand, while COPRA would also overrule any state law that “directly conflicts” with it, it also excludes any state law that “affords a greater level of protection to individuals” from being preempted. This provision causes COPRA to become a federal “floor” of privacy protection, but would give states the freedom to enact its own laws that are more stringent than COPRA. While this approach does have the benefit of states being able to experiment with different privacy protections and those states’ residents benefiting from those protections, it would not solve the problem of legislative fragmentation for tech companies unbounded by administrative borders.

One of the most interesting provisions of COPRA that is not present in the CDPA is the concept of a “private right of action.” This provision would allow any data subject to sue a data controller that is not following the law, instead of leaving that responsibility solely in the hands of the Federal Trade Commission and state governments like the CDPA does. COPRA assumes that any violation of its provisions constitutes a legal injury and allows plaintiffs to sue for $100 to $1,000 *per violation per day*, on top of punitive damages and attorney’s fees, in any state or federal court that has jurisdiction (Kerry and Morris). This has the effect of creating a very effective deterrent against companies violating the law, as they know that any violation would result in a barrage of lawsuits filed against them across the country. Such a clause is not without precedent; a similar clause was included in the Telephone Consumer Protection Act of 1991, where any individual receiving automated telemarketing calls could sue the company for up to $3,000 per repeat violation. As one might expect, this clause is perhaps the most controversial provision in COPRA, with Republicans and moderate, corporate-friendly Democrats opposing its inclusion.

SECTION 3: POTENTIAL TECHNICAL APPROACH TO PRIVACY LEGISLATION

When thinking about how to measure potential threats of data collection and privacy loss, we thought of the Differential Privacy paper. Particularly, because threats to security are not exactly what is being considered here, but rather individual participation in targeted advertising. Considering the normative aspects of a potential privacy threat, we have to also consider the privacy loss of an individual in terms of the population. For instance, in the case of Cambridge Analytica, 87 million user profiles were built, which manipulated democracies(Veliz). Hence, privacy should also be considered beyond the individual basis and Differential privacy evaluates how likely an individual profile could be reconstructed. We consider the relevance of differential privacy in three areas: user segmentation, ad sales, and user profiling.

User segmentation involves narrowing down a larger category of customers into smaller groups, in a way that doesn't reveal individual personal identifiable information. Determining how large to make these user segments can also incorporate a tradeoff. Either, a lot of data can be collected on fewer users for more tailored advertisements, or several profiles with greater ambiguity could be created that would aggregate in order to remain within a privacy budget. Formalizing how differential privacy could affect user segmentation, we consider mathematical definition from PINQ:

$$\mathbf{Pr}[M(A) \in S] \quad \leq \quad \mathbf{Pr}[M(B) \in S] \times \exp(\epsilon \times |A \oplus B|)$$

For two different user segments A and B, how much each additional individual entry affects the overall distribution M is defined by the privacy budget epsilon, the difference in output. Advertisers already face a similar trade-off between how specific ad targeting should be and profitability. The Network Advertising Initiative reported in 2009 that the conversion rate for targeted ads was 6.8%, whereas for traditional ads it was 2.8% (NAI Beales Release). More targeted ads were also twice as expensive, such that advertisers were balancing the cost of increased targeting with the profits from increased conversion.

Having an universal privacy budget for companies and websites would also limit how much data a website collects per user when creating profiles to tailor advertising. The privacy expenditure would need to be considered when specific attributes are being collected about the user for creating user profiles, and determine if the various components are overly identifying. This can prevent more pervasive advertising tactics such as fingerprinting, which involves collecting many web signals that would individually seem meaningless, but together can be identifying.

Lastly, having an universal privacy budget could also quantify the privacy and accuracy trade-off that companies face when selling data to third parties. It could also mean that data is only sold to third parties if enough data was aggregated. For instance, If greater noise and randomization was first used to transform the datasets before being sold or used for targeting advertising, the now anonymous data would be less harmful to an individual.

It is difficult to determine what would be a good privacy budget to choose, to consider both the advertiser and the user. A smaller epsilon would mean increased privacy which would be good for the consumer. However, a smaller epsilon would mean worse accuracy, which would be detrimental to the profitability of an advertisement. A talk at University of Pennsylvania, considers using opportunity cost of participation as another metric (Hsu et al.). For instance the privacy budget would also have to be set according to what an user gains from using a free service, what the cost of not having the service, and how they perceive privacy. Costs of not using a service could even include things like social and cultural capital, and would then be weighted with how much an individual would expect to be compensated. These costs cannot be easily measured objectively, would perhaps involve survey, and would likely vary based on the website. They came up with the equation: $(e^{\varepsilon}P - P) \cdot N \leq B$, for a budget of size B and study of size N individuals. This would then be intersected with the desired level of accuracy, which is also a function of epsilon.

Ultimately, we determined that it would be too difficult of a thing to implement in practice, as it means either a business would have to hire several computer science experts at an inordinate cost, or outsource it to an expensive large company that has the appropriate expertise. This would be an unfriendly policy for small businesses because they would need to somehow quantify the expenditures of each query or each piece of user data collected. To non-experts it would also be difficult to interpret or understand what an epsilon value privacy budget would entail in terms of overall privacy, which would detract from public confidence in a law. Furthermore, it would be difficult to come up with an universal budget that would be applicable in terms of the current service the user is provided and how accurate the advertiser wants the advertisement. It seems as though, allowing for user autonomy of choice in regards to the trade-offs of their data seems more probable. Additionally, if differential privacy was used to transform data before being sold, the receiving party would need to know how to decrypt, and denoise the data, which may not be a realistic implementation.

Section 4. JUSTIFICATIONS BEHIND THE MALTE TREATY'S PROVISIONS

In coming up with the new GDPR, we wanted to balance both what companies had to gain from more specific behaviorally-targeted advertising and what users had to gain with access to information and free services. There is an obvious monetary advantage of having behaviorally-targeted advertising in terms of click-through rates and per ad profitability. Users too may also benefit from seeing products more geared towards their interests. The issues arise from a lack of consumer awareness of data collection, and the potential consequences of that collection. We hope to cover things beyond the scopes of what is currently legally being done to incorporate what should ethically be done to better protect user privacy, while balancing business interests.

4.1. What Each Data Collector is Required to Do

Firstly, targeting advertising should be free of deception. As the American Marketing Association's code of ethics describes, there are six ethical values: Honesty, responsibility, fairness, respect, transparency, and citizenship. In terms of user consent, being free of deception entails full disclosure and granularity of how exactly the company is using user data. This is particularly relevant for how web tracking and third party cookies can be used to create more detailed user profiles in ways that aren't explicit to the user or written in fine text that makes it hard for the average user to comprehend. Therefore, we also believe that user interface designs should have fair promotion of both the consenting and nonconsenting options of allowing for non-essential cookies, without additional nudging. The service should also be functioning to its fullest extent possible if the user chooses to opt-out. By having stricter policies on cookie usage, there will also be greater restrictions on cross-site tracking, making it so that the data being collected on the user is directly related to the service that they are using. These restrictions are particularly important to safeguard user privacy, as there have been instances where social media giants have tracked users across unrelated sites, even those who don't even have an account on that social networking platform (Hern).

Secondly, there should be greater consideration of all stakeholders, or active parties involved. Business Ethics Philosopher Eduard Freeman describes that stakeholders “include any group or individual that can affect or is affected by the achievement of the organization’s objectives.” In terms of targeted advertising, this means having some form of agreement and understanding between all advertising partners, including the DMP and DSPs. For instance, in terms of the Grindr case, there was not enough mutual collaboration among partnerships in order to disclose explicitly how user data was being used. By having the primary service provider be held responsible for defining privacy policies, we hope to mitigate data sharing between different applications without the user’s full acknowledgement.

Lastly, we must take into consideration the potential harm of the data being used. This harm, we decided could not realistically be quantified by privacy loss, because companies would have to have the adequate access to technology. What is considered harm is notably difficult to quantify. According to utilitarianism, to be without harm could be based on happiness, or according to English philosopher John Stewart Mill, “pleasure and freedom from pain”. Pain could be measured both psychologically and on the basis of financial loss. Considering harm from a psychological perspective, certain groups are more vulnerable based on age (young children), or health, but it is also difficult to codify these groups, depending on the type of advertisement. Therefore, we decided to make it such that advertisements about sensitive topics such as politics needed to be shown to everybody, but geographical based advertising is okay without too narrow of a scope.

4.2. What Each User Must Have the Right to Do

Most users are not aware of the breadth of which advertisers are collecting and using data to deliver targeted advertising, or how to limit the advertiser’s ability to track online behavior. We believe that not only should corporations have a duty to act responsibly, but those corporations must give users the right to control how their own data is processed. For instance to further promote user autonomy, the CCPA only allows asking the user to sell data every 12-months. In a new global proposal, we aim to have increased prompting, such that the users are aware of the methods that they can take to make more informed choices about their personal data usage.

We believe that users should also have the right to forget, the ability to get rid of past mistakes or opinions that you may no longer want in the public domain (Veliz). Therefore, if data was collected on the user at some period to indicate that they should be targeted for a particular advertisement, the user should be able to remove the specific information related to that advertisement if their opinions have changed. When a user visits a website, cookies are saved on their computer that can be read by advertisers to auto-generate more tailored ads. Therefore, oftentimes the advertisements that are shown could be outdated and based on prior searches. A woman that is no longer pregnant probably would no longer want to see advertisements for maternity wear. This also entails limiting the amount of third party data, "information collected by an entity that does not have a direct relationship with the user" used to target advertisements with greater precision. Third party data, collected by data brokers, makes it more difficult to determine how specific information is used, and inaccurate information to be corrected, which contradicts the users rights to forget.

Lastly, our new policy functions under a similar presumption as the GDPR that the users have the right to control their data. Idealistically, this also comes with the knowledge that their data is a tradable and commodifiable good such that they are able to decide how they trade it for services. Therefore, there should be methods to delete data from one service, and prevent personal information collected on that service to be used for advertising purposes if that user no longer uses the platform. They should also be fully aware of whether information collected is considered essential to the service.

4.3. Punishments for Violating the Law

No law can achieve its goals without an effective mechanism for enforcement. Our aim in designing a punishment mechanism for violating the law is to create a large enough deterrent so that companies would not even consider taking risks when handling protected data. As we have seen in class from the GDPR case study presentations, many of the fines handed down by authorities to violating companies are nominal in amount, making GDPR fines simply a cost of doing business. In 1968, prominent economist Gary Becker asserted that criminals view the "expected cost of lawless behavior" to be the product of the chance of being caught and the severity of the punishment if caught, and so any punishment should be designed according to this framework (The Economist, citing Becker). To put it in mathematical terms, corporate executives simply evaluate the following inequality, and as long as the left side of the inequality is greater than the right side, corporations have an incentive to break the law despite the consequences:

$$\textit{Potential Profit} > \textit{(Probability of Paying a Fine)} \times \textit{(Potential Monetary Fine)}$$

From a regulator's perspective, it may be tempting to simply increase the two terms on the right side of the inequality as much as possible by ramping up enforcement efforts and instituting extremely large fines. But we must also consider the drawbacks of this approach. Consider a scenario where a company was wrongfully found guilty of breaking the law, or one where a company did break the law but the business itself is fairly small. An inordinately large fine will not have the proper deterrent effect we desire, since a wrongfully convicted company would not have considered the fine at all in its business decisions, and a small business would not be deterred any more with a $500 million fine over a $50 million fine. A 2012 article in The Economist suggests "penalties that offset the benefits of crime," in essence, a fine based on the profits that the criminal behavior generated. This is the approach we have chosen for our treaty. This approach also has the benefit of taking into account some industries have a far lower profit margins than others. It is reasonable to levy different penalties to a billion-dollar airline (with razor thin margins) than a billion-dollar social media company (with much higher profit margins).

However, a government-imposed penalty is not the only way to deter companies from breaking the law. Especially with consumer data privacy laws, there is a discrete, identifiable population that can be harmed by a company's data processing practices. These people deserve a way to force a company to adhere to the law or receive financial compensation. Therefore, similar to how the proposed COPRA creates a private right of action for individuals, our treaty would do the same and allow individuals to sue for liquidated damages themselves. By allowing individuals to sue in their personal capacity (even in a small claims court for an amount trivial for a large corporation), we would increase the first term on the right side of that inequality — the probability of paying a fine. If individuals were empowered to sue for violations of the law on their own or through a class action lawsuit, companies would not only have to fear government prosecution for improper use of data, but also the threat of millions of users holding them accountable as well. At the same time, we want to assuage any fears of mass lawsuits for minor technical violations, as well as protect businesses who have made an honest mistake in handling and processing data. Therefore, we give them a chance to cure any defects in their data processing practices before allowing any lawsuits to proceed.

Finally, we would introduce a third factor to the above inequality that would create a strong incentive to adhere to the law. A corporation is neither sentient nor corporeal, so the only applicable punishment to a corporation is a monetary penalty (or forced dissolution, but that is an extreme result we will not consider at this time). However, a corporation's actions are necessarily carried out by individuals who can be subject to other penalties such as imprisonment. This additional potential punishment would create a strong incentive for those responsible for data processing to act in a responsible manner within the confines of the law, as individual employees and executives may scoff at a fine of a few hundred million dollars to the corporation, but would likely want to avoid personal financial liability or even jail time at all costs. Therefore, in addition to requiring companies to designate a data protection officer much like the GDPR, our treaty would impose criminal penalties on data protection officers acting with negligence or malice.

Convention on Monitoring Advertisers and

Limiting their Targeting Endeavors

(The MALTE Convention)

THE STATES PARTIES TO THIS CONVENTION,

Recognizing

the exponential growth of the Internet in the past several decades

Further recognizing

The growing importance of personal data and the necessity of protecting its abusive usage

Concerned

That the usage of data in irresponsible and reckless ways can result in severe social harm

Noting

The impact of algorithmically targeted advertising on human behavior

Desiring

To regulate the usage of personal data in the context of said targeted advertising

Have agreed as follows:

Article 1

Definitions

1. Any terms of art not explicitly defined in this Convention shall follow the definitions laid out in the text of the European Union General Data Protection Regulation.

2. “Class” shall mean any particular group of users that the Targeted Advertiser is targeting for a specific piece of Targeted Advertising; for example, inhabitants of a particular geographical area, users that have previously shown interest in a particular hobby, political affiliation, etc.
3. “Consumer” shall mean any individual to whom an Advertiser serves Targeted Advertising.
4. “Targeted Advertising” shall mean any form of advertising for a commercial, political, charitable, or personal purpose that is served to the Consumer of an online platform in a selective manner based on data pertaining to the user that the advertiser already possesses.
5. “Targeted Advertiser” or “Advertiser” shall mean any Advertiser that engages in Targeted Advertising.
6. “Protected Class” shall mean membership in a particular social group generally regarded a politically, socially, or culturally sensitive subject matter such as age, race, gender, sex, sexual orientation, political affiliation or opinion, religion, disability status, etc.

Article 2

Duties of Targeted Advertisers

1. A Targeted Advertiser must appoint a Data Protection Officer who shall be responsible for the control, processing, safeguarding, and ensuring the proper use of data that is used to serve Targeted Advertising.
2. A Targeted Advertiser must obtain informed consent from the Consumer to serve such advertising.

   a. Such consent must be given explicitly when the Consumer registers for a platform, or if registration is not a requirement to use a platform, when the Consumer first visits the platform's webpage.
   b. Such consent must be renewed periodically every 3 (three) months.
   c. The Advertiser shall make a substantial effort to educate the Consumer on how and when their data is used to serve Targeted Advertising before asking for such consent.
   d. The Consumer must be able to consent on a granular level; that is, the Consumer shall have the right to opt out of their data being used to serve advertising for a specific purpose, such as by company, industry, political party, etc.
   e. The Advertiser shall draw equal attention to the consenting and nonconsenting options.
   f. The default position of any consent indicator shall be neutral; that is, no selection can be made for the Consumer before the Consumer interacts with the indicator.
3. A Targeted Advertiser must not engage in Cross-Site Tracking of Consumers, defined as the storage or usage of any data gathered from sources other than the Advertiser's full and direct control to serve Targeted Advertising.
   a. This prohibition shall not apply to any Consumers that has already provided explicit consent (to the same standards as Article 2(1)) to be subject to Cross-Site Tracking and who is logged into the Advertiser's platform at that time.
   b. Notwithstanding Article 2(2)(f), explicit consent as meant in this subarticle shall only be given after a default position of nonconsent.

4. A Targeted Advertiser must make accessible the reason as to why a Consumer was targeted for a particular advertisement.
5. Each Targeted Advertiser must have its own privacy policy and shall be liable for all Targeted Advertising that is served on their platform.
6. If the data collected about a Consumer (either a singular piece of information or information in the aggregate) reveals membership in a certain Protected Class, then Targeted Advertising relevant to that Protected Class shall not be served to a Consumer.
    a. There shall be an exception to the prohibition above if the Targeted Advertising relevant to membership in a Protected Class if all individuals within a particularized geographical area have the same likelihood of being served that ad.
    b. This geographical area shall be no smaller than 50 square kilometers.

Article 3

Rights of Consumers

1. A Consumer shall have the right to opt out of Targeted Advertising based on their membership in a Class without opting out of all Targeted Advertising altogether.
2. A Consumer shall have the right to delete any data used to serve Targeted Advertising to the Consumer.
3. A Consumer shall have the right to know what data is being used to serve Targeted Advertising and how it is being used. This data must be available to download within 24 hours of being requested in a human readable and machine readable format.

Article 4

Enforcement of this Convention

1. Any Targeted Advertiser in violation of this Convention shall be levied a fine of no less than 100% but not more than 500% of the profit generated from Targeted Advertising served to Consumers in violation of this treaty.
    a. The exact amount of the fine shall be determined by the courts of each Contracting State.
    b. The percentage of the fine shall be determined taking into account the intentionality and malice displayed by the Targeted Advertiser in violating this Convention.
2. The Consumer shall have a right of action in the courts of each Contracting State to recover damages, both actual and statutory, against an Advertiser serving Targeted Advertising in violation of this Convention.
    a. Such litigation shall only be allowed after the Consumer informs the Advertiser of the violation and the Advertiser does not cure the violation within 30 days of the Consumer's notice.
3. If a Targeted Advertiser is found to have violated this Convention, the Advertiser's Data Protection Officer may be held criminally liable for such violations if said Officer is found to have been reckless, negligent, or malicious in handling their duties.
4. Each Contracting State shall enact legislation allowing for the legal actions described in this Article consistent with the intent to deter violations significantly with monetary penalties and imprisonment time.

Delegation of Work in this Project

The work done in this project was generally split evenly between us two, although there were some parts Rebecca worked on more, due to Hyun's flareup of medical conditions from time-to-time. Research and writing were done individually, but the terms of the new treaty were discussed and decided mutually. The exact breakdown of sections in this report directly written by each of us are as follows. Any duplicated sections between us indicates a joint effort in their direct writing.

Rebecca ● Intro ● 1.1 ● 1.2 ● 1.3 ● 1.6 ● 3 ● 4.1 ● 4.2 (most)	Hyun ● Intro ● 1.4 ● 1.5 ● 2.1 ● 2.2 ● 2.3 ● 4.2 ● 4.3 ● Text of Treaty

Bibliography

Baldwin, Peter, and Lucas Michelen. “New York's New Data Breach Notification Law: What Businesses Should Know.” *The National Law Review*, 3 Apr. 2020, www.natlawreview.com/article/new-york-s-new-data-breach-notification-law-what-businesses-should-know.

Becker, Gary S. “Crime and Punishment: an Economic Approach.” *The Economic Dimensions of Crime*, 1968, pp. 13–68., doi:10.1007/978-1-349-62853-7_2.

Constine, Josh. “A Flaw-by-Flaw Guide to Facebook's New GDPR Privacy Changes.” *TechCrunch*, TechCrunch, 18 Apr. 2018, techcrunch.com/2018/04/17/facebook-gdpr-changes/.

“Cookie Banner Requirements To Meet GDPR and CCPA.” *Red Clover Advisors*, 29 June 2020, redcloveradvisors.com/2020/06/29/cookie-banners-ccpa-gdpr/.

Edelman, Gilad. “'Do Not Track' Is Back, and This Time It Might Work.” *Wired*, Conde Nast, 7 Oct. 2020, www.wired.com/story/global-privacy-control-launches-do-not-track-is-back/.

Fazlioglu, Müge. *COPRA and CDPA: Similarities, Gray Areas and Differences*. International Association of Privacy Professionals, iapp.org/media/pdf/resource_center/COPRA_CDPA_Comparison_WP.pdf.

Fazlioglu, Müge. “Tracking the Politics of US Privacy Legislation.” *Privacy Tracker*, International Association of Privacy Professionals, 13 Dec. 2019, iapp.org/news/a/tracking-the-politics-of-federal-us-privacy-legislation/.

“Fine and Punishment.” *The Economist*, The Economist Newspaper, 21 July 2012, www.economist.com/finance-and-economics/2012/07/21/fine-and-punishment.

Hern, Alex. “Facebook Admits Tracking Users and Non-Users off-Site.” *The Guardian*, Guardian News and Media, 17 Apr. 2018, www.theguardian.com/technology/2018/apr/17/facebook-admits-tracking-users-and-non-users-off-site.

How Do We Apply Legitimate Interests in Practice? UK Information Commissioner's Office, ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/.

How Do We Comply with the Cookie Rules? UK Information Commissioner's Office, ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/.

"The Impact of the CCPA's Do Not Sell Rule on Digital Advertising." *Focal Point Blog*, 21 Nov. 2019, blog.focal-point.com/the-impact-of-the-ccpas-do-not-sell-rule-on-digital-advertising.

Kerry, Cameron F, and John B Morris. "In Privacy Legislation, a Private Right of Action Is Not an All-or-Nothing Proposition." *Brookings Institute*, Brookings Institute, 7 July 2020, www.brookings.edu/blog/techtank/2020/07/07/in-privacy-legislation-a-private-right-of-action-is-not-an-all-or-nothing-proposition/.

Norway, Forbrukerrådet [The Consumer Council of Norway], *Out of Control: How Consumers Are Exploited by the Online Advertising Industry*, 14 Jan. 2020. fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf.

Porter, Jon. "Grindr Shares Personal Data with Ad Companies in Violation of GDPR, Complaint Alleges." *The Verge*, The Verge, 14 Jan. 2020, www.theverge.com/2020/1/14/21065481/grindr-gdpr-data-sharing-complaint-advertising-mopub-match-group-okcupid-tinder.

Schultz, David. "Telemarketing." *The First Amendment Encyclopedia*, Middle Tennessee State University, 2009, www.mtsu.edu/first-amendment/article/1151/telemarketing.

Shiffman, Eric. "What Is Third-Party Data?" *SpotX*, 6 Mar. 2020, www.spotx.tv/resources/blog/product-pulse/what-is-third-party-data/.

South Korea, Korea Communications Commission, *온라인 맞춤형 광고 개인정보보호 가이드라인 [Guidelines for Personal Information Protection in Online Personalized Advertisements]*, Feb. 2017. policy.nl.go.kr/cmmn/FileDown.do?atchFileId=220309&fileSn=61723.

South Korea, Ministry of the Interior and Safety, 이재구. *2019년 개인정보 보호법 위반사례 및 대응방안*, Personal Information Protection Commission, 2019. privacy.go.kr/cmm/fms/FileDown.do;jsessionid=6J7O7kT-P2l34Rqb5vesmcGj.PVCserver2?atchFileId=FILE_000000000837290&fileSn=1.

United States, Congress, Mulligan, Stephen P, et al. *Data Protection Law: An Overview*, Congressional Research Service, 25 Mar. 2019. fas.org/sgp/crs/misc/R45631.pdf.

Van den Brande, Bart. "Is Targeted Advertising a Form of Automated Decision Making under Article 22 of the GDPR?" *Sirius Legal*, 2 Jan. 2018, siriuslegaladvocaten.be/is-targeted-advertising-a-form-of-automated-decision-making-under-article-22-of-the-gdpr/.

Villi, Dario. “GDPR and Facebook: All You Need to Know to Keep Advertising Safely.” *LeadsBridge*, LeadsBridge, 26 Feb. 2020, leadsbridge.com/blog/guides/gdpr-and-facebook-all-you-need-to-know-to-keep-advertising-safely/.

Véliz, Carissa. “The Internet and Privacy.” *Ethics and the Contemporary World*, 2019, pp. 149–159., doi:10.4324/9781315107752-12.

“What Is a First-Party DMP?” *Kevel*, adzerk.com/blog/first-party-dmp/.

What Is the 'Legitimate Interests' Basis? UK Information Commissioner's Office, ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/.

Wlosik, Michal. “What Is a Data Broker and How Does It Work?” *Clearcode Blog*, Clearcode, 25 Nov. 2020, clearcode.cc/blog/what-is-data-broker/.

김윤희. “개인정보 유출 사고 나면 기업 대신 직원만 속 탄다.” *ZDNet Korea*, 11 Oct. 2019, zdnet.co.kr/view/?no=20191011083159.

전규향. “개인정보보호법 [Personal Information Protection Act].” *KCLA Monthly Journal*, Feb. 2012, pp. 122–125., www.klca.or.kr/KLCADownload/eBook/P7622.pdf.