EXECUTIVE SUMMARY

In January 2017, the European Union published the much anticipated draft Privacy and Electronic Communications Regulation ("ePrivacy Regulation") to replace the current Privacy and Electronic Communications Directive ("ePrivacy Directive") and govern the processing of electronic communications data and collection of data from user devices in the Big Data era.¹ If adopted, the ePrivacy Regulation would impact the entire online advertising ecosystem, but most dramatically the businesses of data juggernauts Facebook and Google, which have not been subject to similar regulatory requirements in the past.

Under the new draft Regulation, Facebook and Google would be required to obtain more clearly demonstrable consent from their users prior to processing any data (not just personal data) for online behavioral or targeted advertising purposes and, in some instances, would be completely barred from processing data for such purposes. The steps required by the current draft Regulation for Facebook and Google to obtain the requisite consent would require an overhaul of their current practices and would likely significantly curtail the scale at which they collect data. Should they fail to update their privacy practices in a more consumer-friendly way as required by the draft Regulation, Facebook and Google will either be (a) prohibited from using the unprecedented amounts of data already in their control; or (b) subject to fines and penalties that will, for the first time in history, have a significant impact on their bottom lines. Based on their reported revenue in 2016, Facebook and Google could face annual fines up to $1.07 billion and $3.58 billion, respectively.

At the same time, companies that collect and use data at smaller scale (such as solely on their owned and operated domains) are likely to be less impacted by this Regulation. These companies will be significantly less challenged in getting the required consent for their limited purposes. As a result, companies that create trusted, premium digital experiences, enjoy direct relationships

¹ The draft ePrivacy Regulation is available at https://tinyurl.com/grcegr7. On September 8, 2017, the Council of the European Union proposed revisions to the ePrivacy Regulation, available at https://tinyurl.com/yddvgrbx
with consumers and do not rely on tracking consumers at such a large scale may find new leverage and opportunities in the marketplace.

BACKGROUND

Facebook and Google are the two biggest players in the online advertising ecosystem.\(^2\) They primarily monetize their services through the placement of ads directly on their online platforms as well as through technology embedded on third party publisher websites and apps. Facebook allows advertisers to place ads on its social media newsfeed and columns, on its associated platforms (including Instagram and Facebook Messenger), and on third party websites and apps that are part of the Facebook Audience Network. Likewise, Google allows advertisers to place ads on its Google owned services, including Google Search, Gmail, and YouTube, as well as on third party websites and apps that use Google’s ad serving technology services, such as DoubleClick and AdSense.

While Facebook and Google are based in the U.S., their businesses span across international borders, including into the European Union (“EU”). The EU has different laws and regulations than the U.S., and the EU privacy legal regime treats individual privacy as a fundamental human right. In the past, EU regulators have brought actions against Facebook and Google for alleged privacy violations, but have not had the regulatory teeth to impose severe penalties on either company. One notable recent example is the nominal fine of 150,000 EUR imposed by French regulators in May 2017 as a result of actions taken by French and Dutch regulators against Facebook for alleged violations of those jurisdictions’ data protection rules.\(^3\)

The EU adopted the General Data Protection Regulation (“GDPR”) in 2016 to replace the current Data Protection Directive (“DPD”) and govern the processing of personal data of individuals located in the EU. The GDPR will become effective in May 2018 and includes extraterritorial jurisdiction provisions designed to reach companies that are not based in the EU but that process data about individuals in the EU (such as Facebook and Google). Notably, the GDPR will allow regulators to fine companies up to four percent of their total annual turnover of the preceding financial year.

In addition to the already looming GDPR effective date, EU policymakers have proposed the draft ePrivacy Regulation to replace the current ePrivacy Directive and govern the processing of electronic communications data. The ePrivacy Regulation is intended to “particularise and complement” the GDPR, and, if adopted, would become binding law across the EU as early as May 2018. Similar to the GDPR, the ePrivacy Regulation is written to facilitate the exercise of jurisdiction over companies that are not based in the EU but that process electronic


communications data or collect device data from users in the EU. The fines mirror those in the GDPR, meaning the ePrivacy Regulation has teeth.

The ePrivacy Regulation is controversial as it prohibits the processing of electronic communications data and collection of data from user devices absent an exception, which could destroy the ability of companies to monetize content through online behavioral or targeted advertising. As the two biggest players in the online advertising ecosystem, Facebook and Google have the most to lose. This paper analyzes the potential impact of the ePrivacy Regulation on Facebook and Google.

ANALYSIS

- **Facebook and Google dominate the online advertising ecosystem because they have unrivaled access to user data.**

Facebook and Google sit on incredible amounts of user data and are able to leverage that user data to serve highly targeted ads to users. Advertisers can target users based on a variety of data points, such as location, age, gender, language, interests, behaviors, and demographic information. Further, advertisers can upload their own customer list data to Facebook and Google services (such as email addresses, phone numbers, user IDs, and mobile ad IDs), and use the services to identify and serve ads to those customers as well as to other similar users. Facebook even allows advertisers to embed Facebook tracking technologies on their own websites and apps, and serve ads to any users who visit those websites and apps as well as to other similar users as identified by Facebook. These targeted ads are extremely valuable, with one study published by the Network Advertising Initiative over seven years ago finding them to generate 2.68 times as much revenue per ad as non-targeted ads.  

Facebook and Google accumulate these vast troves of user data through their unequalled number of consumer-facing, first party touchpoints. As of June 2017, Facebook had over two billion monthly active users on its social media platform.  

Facebook Messenger and WhatsApp each have 1.2 billion active users, and Instagram has 700 million active users. As of May 2017, Google had seven services that each had more than one billion users, including Google Search, Gmail, YouTube, Chrome, Google Maps, Google Play, and Android. Google Drive has 800 million users and Google Photos has 500 million users.

---


These numbers increase exponentially with the addition of less apparent touchpoints where Google and Facebook act as a third party on a website or app, such as Facebook Login, Facebook Like Button, Facebook Custom Audience, Google Analytics, Google DoubleClick, and other technology services. According to a 2016 census of the top one million most visited websites on the Internet, Facebook is present on more than 35% of those websites, and Google is present on more than 85% of those websites. Further, Facebook and Google own all ten of the top ten domains embedded on or linked to those websites. Indeed, out of 81,000 companies with domains found within the surveyed websites, Google and Facebook (as well as Twitter) were the only companies with domains appearing on more than ten percent of those websites.

Through each of these touchpoints, Facebook and Google glean various pieces of information about their users, which can be combined (both internally and with data from third parties) to create holistic and robust data profiles of their users. These various pieces of information may come from information voluntarily submitted by users (such as when registering an account or contacting customer support) or collected through invisible tracking technologies (such as embedded pixels, dropped cookies, GPS technology, and device fingerprinting) on the services. Common pieces of information include names, email addresses, phone numbers, dates of birth, gender, photos, messaging content, email content, biometric data, device identifiers, location, and browsing behavior.

- **Facebook and Google have set their own rules for privacy.**

Facebook and Google have been able to accumulate massive amounts of user data under existing environments. As discussed above, the EU recognizes online privacy as a fundamental right, but historically has lacked the ability to impose significant penalties for privacy violations. EU regulators have even turned to antitrust regulation rather than privacy law to issue penalties against Facebook and Google. For example, in May 2017 the EU fined Facebook $122 million for combining data from its social media platform with data from WhatsApp after it represented during the acquisition process that it would not combine the data.

Facebook and Google have required users to agree to online policies that permit the companies to share data among and across their services and process data for advertising purposes. By way of example, Facebook requires users to agree to the following language when signing up for a free account: “By clicking Create Account, you agree to our Terms and that you have read our Data Policy, including our Cookie Use.”

---


Facebook and Google take the position that this constitutes consent for all of their processing activities, including services offered outside of their online platforms and embedded on third party websites and apps. And this position works well for Facebook and Google. The companies have so many users that virtually any consumer who comes into contact with Facebook and Google services outside their platforms will have already agreed to Facebook and Google policies allowing for the processing of data through such services.

- **The ePrivacy Regulation would prohibit Facebook and Google from processing for online behavioral or targeted advertising purposes electronic communications data or collecting or accessing device data based on their historic approach to user “consent.”**

The ePrivacy Regulation would impose restrictions on data processing that go far beyond what Facebook and Google have dealt with in the past, in particular because it would allow regulators to fine them up to four percent of their total annual turnover of the preceding financial year. There are several key provisions that would directly limit the ability of Facebook and Google to process user data for online behavioral or targeted advertising purposes.

- Facebook and Google would not be able to process electronic communications data unless an exception applies (usually involving consent, discussed in detail below). Electronic communications data is broadly defined as data related to electronic communications services, such as instant messaging, email, and Voice over IP services. It includes both the content of a communication (such as the words within a text message or voice content within a call) and the metadata within the communication (such as underlying information about the device, time, and location of use). It appears that even content and metadata related to a Facebook “Like” or share would constitute electronic communications data.

- Unless an exception applies, Facebook and Google would be required to erase or anonymize any electronic communications (a) content after receipt; and (b) metadata when it is no longer needed for the purpose of the transmission of a communication.

- Facebook and Google would be prohibited from collecting information from or accessing information on any user’s terminal equipment (including any device, laptop or phone) unless an exception applies.

These prohibitions would apply to nearly all Facebook and Google services including instant messaging, email, and Voice over IP, and would apply to the companies’ own platforms and their activities using third party tracking technologies embedded on websites and apps. In order to continue providing their services, Facebook and Google would need to qualify for an exception. Consent is the only plausible exception for most online behavioral or targeted advertising activity.

- **User consent is the exception under the ePrivacy Regulation that would allow Facebook and Google to continue processing information for online behavioral or targeted advertising purposes in some circumstances.**
The ePrivacy Regulation provides a limited number of exceptions to its blanket prohibition on data processing. Of those exceptions, there are only a subset of exceptions that would allow Facebook and Google to process data for online behavioral or targeted advertising purposes. The common thread in most of these exceptions is that they require user consent. Facebook and Google could:

- process electronic communications content if they demonstrate (i) consent from all users concerned for the specified processing purpose; (ii) the purpose could not be fulfilled by anonymous data; and (iii) either they previously consulted with a supervisory authority OR the sole purpose of the processing is to provide a specific service to the user.

- process electronic communications metadata if they demonstrate (i) consent from the user for the specified processing purpose; and (ii) the purpose could not be fulfilled by anonymous data.

- store electronic communications content or metadata if they are subject to one of the exceptions above.

- collect information from or access information on a user’s device if they demonstrate (i) the user has given consent for the collection or access; or (ii) the collection is necessary for web audience measuring, provided such measuring is carried out by the provider of the service or by a third party on behalf of the service provider subject to compliance with conditions set forth in the GDPR.

- collect information emitted by terminal equipment of the user to enable it to connect to another device or to network equipment if they demonstrate (i) the user has given consent for the collection; (ii) they provided a clear and prominent notice of the collection along with options for the user to stop or minimize the collection; and (iii) they applied security measures appropriate to the risks.

For the most part, with user consent, Facebook and Google could process and store electronic communications metadata and collect information from or access information on a user’s device for online behavioral or targeted advertising purposes. However, Facebook and Google may have difficulty demonstrating that the processing purpose could not be fulfilled by “anonymous” data. The ePrivacy Regulation does not define the term “anonymous,” and making personal data (broadly defined to include even dynamic IP addresses) anonymous is practically impossible from an EU regulator perspective.\(^\text{10}\)

\(^{9}\) The exception in (ii) is of little help to Facebook and Google. Although Facebook and Google could collect information for data analytics purposes, they could not use such information for online behavioral or targeted advertising purposes.

• In some circumstances, Facebook and Google may be prohibited from processing electronic communications data for online behavioral or targeted advertising purposes.

Notably, there appears to be no standalone consent exception under Article 6(1) for the processing of combined electronic communications content and metadata. Further, the Regulation may pose an insurmountable challenge for targeted advertising based on the content of instant messaging, email and Voice or IP services. This seems unavoidable given the high bar for obtaining consent for specified purposes. The need to obtain consent from all users, and the requirement to consult with a supervisory authority in order to process electronic communications content for online behavioral or targeted advertising purposes. This may mean that Facebook and Google may not be able to process the actual content within any messages, emails, calls, and even posts for online behavioral or targeted advertising purposes. Although arguably the result of other legal forces currently at work in the US, Google may already be gearing up for the potential impact of the ePrivacy Regulation as it recently stopped scanning content in user Gmail accounts for online behavioral or targeted advertising purposes.11

• The consent currently received by Facebook and Google from their users would not be sufficient to meet the standard of demonstrable consent required by the draft ePrivacy Regulation.

The ePrivacy Regulation defines consent as the “conditions for consent provided for” in the GDPR. Under the GDPR, consent requires a company to demonstrate a clear affirmative act by the user establishing a freely given, specific, informed, and unambiguous indication of the user’s agreement to the processing. If a company seeks consent for multiple matters, it must present a request for consent “in a manner which is clearly distinguishable from the other matters.” Consent may not be considered freely given if it is conditional on the processing of personal data that is not necessary for performance of the contract. While final EU guidelines for consent have not been released, the consent currently received by Facebook and Google from their users would not constitute a clear affirmative act establishing specific, informed, and unambiguous indication of a user’s agreement for processing personal data (which is broadly defined under the GDPR to include any information relating to an identified or identifiable natural person including location data or any online identifier).

Further, under the draft Regulation, a user must be able to refuse or withdraw consent at any time and without detriment, and shall be reminded of such right to withdraw consent at least once every twelve months for as long as the processing continues.

From a practical perspective, this means that Facebook and Google would not be able to rely on any prior or prospective consent bundled with the use of their services. Facebook’s disclosure language discussed above would not suffice. Rather, Facebook and Google would need to implement new methods for obtaining demonstrable consent, such as through a series or menu of checkboxes upon sign up that users could individually agree to or reject regarding the purposes

for processing data, including online behavioral or targeted advertising. Further, Facebook and Google would still be required to offer their services to users who decline to opt-in to the processing of their data for online behavioral or targeted advertising purposes, as well as provide withdrawal options and regular reminders to users who choose to opt-in.

- **The inability of Facebook and Google to meet the consent requirements under the ePrivacy Regulation could destroy their ability to collect meaningful data at scale in the EU.**

Under the proposed ePrivacy Regulation, much of the EU data subject data on which Facebook and Google currently sit could lose its value because it could not be used for online behavioral or targeted advertising purposes, without dramatic changes to their current practices. Without the implementation of new more robust consent mechanisms, they could not process the metadata within any messages, emails, calls, or posts for online behavioral or targeted advertising purposes; and they could not collect or access any information from user devices or place tracking technologies (such as cookies) on user devices for online behavioral or targeted advertising purposes. And without such fundamental changes to their model, the ePrivacy Regulation would likely eliminate Facebook’s and Google’s ability to match customer list data against their own data and target users on and off their platforms, essentially stripping much of the value associated with the placement of their third party technology on websites and apps. Clearly, the scale at which Google and Facebook collect consumer data would be significantly curtailed.

Even Facebook and Google would feel the impact of fines of up to four percent of their total annual turnover of the preceding financial year. Facebook’s annual turnover for 2016 was $27.64 billion while Google's annual turnover for 2016 was $89.46 billion, meaning the companies could face fines up to $1.07 billion and $3.58 billion, respectively.

- **The ePrivacy Regulation is a greater threat to Facebook and Google than the GDPR.**

Although the ePrivacy Regulation is intended to “particularise and complement” the GDPR, it differs in a number of respects that may prove more problematic for Facebook and Google than the GDPR.

The first key difference is that the ePrivacy Regulation would only allow Facebook and Google to process electronic communications data for online behavioral or targeted advertising purposes based on user consent while the GDPR provides additional bases for processing of personal data. Under the GDPR, a company may process personal data on the basis of its legitimate interest except where such interests are overridden by the interests or fundamental rights and freedoms of the user, and the legitimate interest exception could arguably apply to certain types of targeted advertising.

Another key difference is that the ePrivacy Regulation governs data not covered by the GDPR and would restrict Facebook and Google from processing data they could otherwise process under the GDPR. The GDPR governs the processing of “personal data,” defined as information relating to an identified or identifiable natural person. By contrast, the ePrivacy Regulation
broadly governs the processing of any electronic communications data or data related to the devices of natural or legal persons, including both personal data and non-personal data. Further, the Recitals in the ePrivacy Regulation provide that the Regulation governs the transmission of machine-to-machine communications related to the user and extends to services that include an ancillary communication functionality. Putting these provisions together, the ePrivacy Regulation could conceivably prohibit any data transmissions by Facebook or Google between connected IoT devices.

One other difference worth noting is that, unlike the GDPR, the ePrivacy Regulation does not include a definition of pseudonymized data. Under the GDPR, pseudonymized data is a middle ground between personal data and anonymized data, and the option to pseudonymize may provide companies with some flexibility regarding the de-identification of personal data. As discussed above, Facebook and Google may have difficulty meeting requirements regarding “anonymous data,” especially as making data anonymous is practically impossible from an EU regulator perspective.

- **The ePrivacy Regulation is not yet in effect, but change is coming.**

The draft ePrivacy Regulation as proposed (including with the September 2017 revisions) clearly poses challenges for the online advertising ecosystem, and particularly threatens the scale of data collection by Facebook and Google. Hundreds of stakeholders have already submitted comments on the proposed Regulation, and EU policymakers are expected to review these comments and vote on the proposal later this year. It is quite possible that the language in the final Regulation will differ from that of the current draft. No matter what happens, it is highly likely Facebook and Google will need to make major changes to their online behavioral and targeted advertising practices in order to comply with forthcoming EU privacy laws and regulations.