Google Made an Example in GDPR by French CNIL

The new General Data Protection Regulation (GDPR)—passed on May 25, 2018—is likely to drastically change the way that data-driven companies are allowed to do business in Europe and possibly abroad. While before companies could bury the data processing clauses deep inside the contract and have all the permissions be pre-ticked, GDPR is putting a stop to that, insisting on consumer information and company transparency.

The case that provides the best evidence for this is the recent Google case. The French data watchdog, *Commission National de l'Informatiques et des Libertés* or CNIL for short, received the first complaints against Google regarding GDPR within the first couple of days following the passing of the said regulation. Two advocacy groups lodged the complaints against Google: La Quadrature du Net and None of Your Business. La Quadrature du Net submitted the complaint on behalf of 10,000 individuals, as it would have been too complicated for each of the individuals to do it themselves (Euronews, 2019).

On January 21, 2019, the CNIL finally took a decision and fined Google 50 million Euros for lack of adequate information and transparency as well as lack of valid consent. Even though a 50 million Euros fine may seem like a lot—and this was indeed the largest fine that the CNIL had ever given—Google could have actually had it a lot worse. Under GDPR, companies can be charged up to 4% of their global revenues for any infringement, which is particularly dangerous for companies with a profit margin less than 4%. Given that Google made 34 billion Dollars in the last quarter of 2018 alone, the company could have easily been fined in the billions of dollars if the CNIL saw reason to do so (Porter, 2019).

Nonetheless, Google is confident that it has followed all the rules. The company insists that "people expect high standards of transparency and control from us. We're deeply committed to meeting those expectations and the consent requirements of the GDPR" (Vinocur, 2019). As a result of this commitment, the company believes that it has done nothing wrong and plans to appeal the CNIL decision to avoid creating a precedent for the future and to protect other smaller companies who might not be able to survive a fine from CNIL on data privacy.

First Infringement: Lack of information and transparency

The first major concern that the advocacy groups signaled and that the CNIL took issue with is the lack of transparency. The CNIL said in a statement that:

> *"Indeed, the general structure of the information chosen by the company does not enable to comply with the Regulation [GDPR].* ***Essential information****, such as the data processing purposes, the data storage periods or the categories of personal data used for the ads personalization,* ***are excessively disseminated across several documents****, with buttons and links on which it is required to click to access complementary information.* ***The relevant information is accessible after several steps only****, implying sometimes up to 5 or 6 actions." (The Local, 2019)*

Here the CNIL takes issue with the fact that the information is spread out over several pages instead of being expressly stated on the contract page. Consequently, the user must dig through all of the pages related to the contract and actively take steps in order to get all the relevant information. This hinders one of the two main points of the GDPR: transparency. As is stated in recital 39 of GDPR, "The

principle of transparency requires that any information and communication relating to the processing of those personal data be **easily accessible** and easy to understand, and that clear and plain language be used." Having to click through a handful of pages clearly does not make the information "easily accessible." Google's way of showing the contract purposefully hides information in order to discourage the user from combing through all of it and being well informed. Additionally, bits and pieces of the information are spread out and repeated in several locations, a strategy that serves simply to tire out the consumer and to make them give up in order to simply agree to the terms presented to them without actually reading the whole agreement.

The contract that the user must agree to is broken down into multiple sections: the consent page initially provided, the Privacy Policy[1] and the Terms of Service[2], both mentioned on the consent page and referenced with hyperlinks. In order to get to the Privacy Policy page with the aim of getting more detail than offered on the initial consent page, the user needs to specifically click on a hyperlink to navigate away from the consent page for their new Google Account in the hopes of getting a better understanding of the basis of the contract that they are deciding whether to accept or not. This is yet another barrier to transparency as moving away from the contract page poses extra effort from the side of the user. What's more, the user runs the risk of having their application time-out while they navigate away from the consent page, thus forcing them to start the whole account application process all over again. Therefore, it is very unlikely that the user will actually ever make it to the Privacy Policy page and will thus never be exposed to the entirety of the contract that they are signing. This spreading of information over several pages is expressed by the CNIL and is one of the reasons why the organization believes that Google has not met the requirement of transparency under GDPR. Thus, the structure of the contract does not fulfil the transparency clause of the GDPR and must be changed if Google wishes to continue to have operations in Europe.

Moreover, due to the nature of Google's services, the company must take more effort to explain the extent to which personal data is being gathered and compiled. The CNIL states that:

> *"Users are not able to fully understand the **extent of the processing operations** carried out by Google. But the processing operations are particularly massive and **intrusive because of the number of services offered** (about twenty), the amount and the nature of the data processed and combined. The restricted committee observes in particular that the purposes of processing are described in a too **generic and vague manner**" (The Local, 2019).*

As a result, Google does not sufficiently inform the user of the extent to which their data will be processed. Due to the vague language, Google is not being transparent with their processing operations, which is in violation of GDPR, according to recital 60:

> *"The principles of **fair and transparent** processing require that the data subject be **informed of the existence of the processing operation and its purposes**. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account **the specific circumstances and context in which the personal data are processed**."*

Google fails to satisfy this clause in the GDPR given that it fails to mention all the services that it offers and how it compiles the data gathered from them. Reading through the Terms of Service and the

[1] https://policies.google.com/privacy?hl=en
[2] https://policies.google.com/terms?hl=en

Privacy Policy, YouTube is the sole service that is mentioned by name: “Google may show you ads based on your activity in Google services (search or YouTube for example), as well as on Google's websites and partner apps.” Given that YouTube has its own permissions specified in the contract, mentioning YouTube as one of Google’s services does not provide the user with more insight on the many services that Google provides and from which it collects data. Also, search is Google’s main service so mentioning it does not provide any additional information to the user. By not bringing up any extra services, Google is actively limiting the user’s perception on how much data is really collected on them and from where it is being obtained. This limits the user’s understanding of how much Google knows about their personal life.

The rest of the statements mentioning Google’s many services are simply vague statements that Google offers multiple services and that the data gathered from all those services will be compiled: “We may combine the information we collect among our services and across your devices for the purposes described above”. These types of statements are not transparent as the user is not informed of the “services” or “devices” that Google is referring to, nor are they given any specifics about the “purposes described above”, which are all vague statements relating to collecting data for the proper functioning of the services and for ad personalization. Therefore, Google does not fulfill the GDPR requirement of giving “the specific circumstances and context” of the company’s data processing.

The two statements above were found in two *different* sections of the Privacy Policy, showing the repetition of vague language and the lack of specific information. This lack of transparency and specific information leads to more issues for Google and its users. If the users are not well informed, then, by default, they cannot give valid consent.

Second Infringement: Lack of adequate consent

As mentioned above, due to the information being spread out over several documents and the fact that the purposes were not specific at all, the user does not have enough information to give their valid consent. Therefore, if Google does not have valid user consent (and because it does not have public interest or legitimate interest), the company does not have a legal basis for the processing of European data under GDPR.

In addition to providing users with the specific purposes of how their data will be used, according to recital 39 of GDPR, companies are required to provide the users with the amount of time for which their data will be kept. This amount of time should not exceed what is necessary in order to process the data:

> *“This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. […] In order to ensure that the personal data are not kept longer than necessary,* ***time limits should be established*** *by the controller for erasure or for a periodic review”* (GDPR recital 39).

Unfortunately, Google did not provide this time limit to users in its permissions descriptions. The only mention of time in the Privacy Policy or the Terms of Service is: “In some cases, we retain data for limited periods when it needs to be kept for legitimate business or legal purposes”. This statement is very vague as it does not give the user any indication of what those cases may be and how long the “limited period of time” is. Due to the words employed, the statement is devoid of any real meaning for the user and again fails to meet the guidelines set up by GDPR. What’s more, in the following line, there is a link for more information on “data retention periods.” This link leads to yet another section

on the Google *Privacy and Terms* website: Technologies. In this section, there is an entire page dedicated to explaining how data are different and have different retention periods. However, due to the vague and noncommittal nature of all the language on the *How Google retains data we collect* page in the Technologies section, no more information can be gleaned from this entire page than from the short statement on the Privacy Policy page mentioned above. Moreover, neither the Technologies section nor the page on data retention are mentioned anywhere on the consent page. So, if we consider the consent page (i.e. the only page that is definitively shown to the user) as the contract, not only is there no information about retention period in the contract, but there are no references to it anywhere in the contract, as the Privacy Policy and Terms of Service have at the very least been. To sum up, not only is the information about the retention period just as vague as the information in the other sections, but it is technically not even in the Google Account contract. As a result, future users cannot give adequate consent to Google to process their data as they do not have all of the necessary information to make that decision.

Furthermore, under GDPR, users should have to opt-in to giving their data, not opt-out of it. Consequently, the fact that some of the permission boxes were pre-ticked inherently infringes on the opt-in mechanism. As explained by CNIL in their statement: "as provided by the GDPR, consent is 'unambiguous' only with a clear ***affirmative action from the user*** (by ticking a non-pre-ticked box for instance)" (The Local, 2019). Except for the Location History and the Voice and Audio Activity permissions, all the rest were pre-ticked and thus do not allow for "affirmative action from the user." Not only that but they were hidden behind a "More Options" drop-down (see Appendix), making the process of opting out significantly more difficult than opting in, something that is specifically forbidden in GDPR. Additionally, in the Privacy Policy, it is stated that "You also have the right to oppose the processing of your information or to export the information to another service." Yet, there is no explanation as to how a user could take such action, again making opting out more difficult than the automatic opt-in scenario.

Finally, the consent could be said to be "forced consent" as the user is not informed of the consequences of not giving their consent (AFP, 2019). This is in clear violation of GDPR, according to recital 60:

> *"Where the personal data are collected from the data subject, the data subject* ***should also be informed whether he or she is obliged to provide the personal data and of the consequences****, where he or she does not provide such data."*

Due to the hidden and pre-checked nature of the consent boxes, the user is only given the option to opt-out and is made to believe that they must give their consent if they wish to use the services. Here again, the user is not able to give their valid consent as they are not informed that it is not required to provide all the requested personal data and that they have the choice to simply opt-out.

To conclude, due to reasons of vague and non-specific purposes, missing retention periods, the opt-in nature of the permissions and the fact that the consequence of not giving permissions are not explained, the user cannot give their *valid* consent and thus Google does not have a legal basis for collecting the personal data of European users under GDPR.

Google's response and implications

Google, though, does not agree with CNIL. One of the reasons given for this dissent is that fact that the company believes that GDPR should only be applied to the French site (i.e. Google.fr) and not to

its global services and sites, which are based outside of France and more generally Europe (AFP, 2019). As a result, Google has decided to appeal the decision.

Even if Google happens to be successful with this argument, it might not protect the company's operations for long. The United States seem to be moving more and more to the European model of data protection. In 2018, California passed the California Consumer Privacy Act, which is similar to GDPR in that it aims to protect consumers and their data from large corporations (Gaus, 2019). The US government is likely to create a federal law that will supersede the state laws on consumer privacy in order to keep some consistency in the law and simplify the regulations with which companies need to comply. This law is expected to look something like GDPR and is likely to come sooner rather than later due to the numerous data scandals over the past couple of years, including the very recent Facebook private message scandal at the end of 2018 (Sandal, 2018).

A move closer to GDPR and away from the individualistic nature of data protection in the US could likely lead to more data protections and less data breaches. However, it could also lead to less innovation and differentiation by companies which can hinder the growth of the American economy. This is due to the fact that data-driven companies get their value added from their large data investments. As a result, if those companies no longer have current databases on consumers, they will not be able to offer new services that the consumers will appreciate.

If companies were to invest more money in data encryption and protection in order to ensure that, even if data is leaked, it will not be readable and will therefore not be able to be used in any malicious way, stricter regulations, such as GDPR, might not be necessary in the US. Until now, multiple companies have failed to encrypt the data they collect from consumers because it costs money and will thus hurts their bottom line in the short-term. One example of such a decision is Amazon Ring, which recently dealt with a data breach where employees viewed live stream of customers' security cameras (Fedorenko, 2019). This example shows that investing in data encryption and protection could yield large returns in the future, in the form of a saved PR scandal and a more lenient consumer data protection law. In Europe, GDPR already provides for this data protection. According to article 32, companies need to take the necessary steps for data protection by requiring processes such as "pseudonymisation and encryption" to ensure that data is not used for malicious reasons. American companies can take note of this regulation guideline to reduce the negative impact of data breaches in the hopes of avoiding the need for a strict data protection regulation in the US and thus allowing companies to keep their data-driven differentiation business model. When doing business in the European Union though, they will have to adapt their operations to GDPR.

Other Aspects of Google's Privacy and Terms

According to the Privacy Policy, Google aims to take all the necessary steps in protecting consumer data. The company "encrypts your data to ensure confidentiality in the context of transfers" and limits the access to user data "to Google employees, contractors and agents who need to access it in order to process it on our behalf. Anyone with access to it is subject to strict confidentiality obligations and may be subject to disciplinary sanctions." While the company could obviously do more, it seems to be fulfilling the requirements set forth by the abovementioned article 32 of GDPR. Thus, Google takes both technical and legal actions—assuming that "strict confidentiality obligations" means the signing of a Non-Disclosure Agreement—to protect the user data.

When it comes to transferring data, Google works "with trusted companies that act as 'data processors' and not partners, that is, they process the information on our behalf to enable us to

provide our services, as per our instructions." This data transfer is permitted without the consent of the user under GDPR because the third-party is acting in the place of Google and is not using the data for its own purposes.

In addition to third-party processors, other third-parties—that Google refers to as "Partners"—have access to user data from Google services. Google however does not create a data lake and license the data to the third-parties. Instead, Google "allows specific partners to use their own cookies or similar technologies to collect information contained in your browser or device for advertising and evaluation purposes", according to the Privacy Policy. Again, there is no specific description of who those partners are or what the specific purposes are. What is important is that those unnamed partners collect the data themselves. As a result, while Google collects the data and records the unique personal identifiers that go with the data, the third parties are only allowed to collect anonymized measurements from some of the Google services. By not creating a shared data lake but instead creating a private database, Google is in a way protecting the personal privacy of the individual users. Additionally, because the Partners' data is anonymized, they are not liable under GDPR. This holds true as long as they do not use this data to create some sort of model and then try to profile any future European customers without their express consent.

In the same style as the rest of the contract, Google's explanation of how the data that it has gathered on users will be transferred in the case of a change in ownership is rather vague. In the Privacy Policy, it states that "If Google is involved in a merger, acquisition or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy." With this statement, Google is announcing to the user that if something were to happen to the company, their data will simply be sold off to another and that Google will notify the users if this becomes the case. Google has the authority to make such statement as it postulates in the Terms of Service that "using our Services does not give you ownership of any intellectual property rights in our Services or the content you access." For Google, all the services and data created using those services is the company's intellectual property. As a result, by signing the contract, the user relinquishes all owner rights to the data and measures collected on them. This makes Google the owner of the database filled with user data and it can therefore sell that data to anyone else. It is also for this reason that Google has the liberty to use a user's name and photo along with their online review about a company in an ad for that company, without asking the permission from the user. Even though the user is the author of the review, Google is the owner and can do whatever it wants with it.

That being said, any data uploaded to Google services by the user remains the intellectual property of the user: "Some of our Services allow you to upload, submit, store, send or receive content. You retain ownership of any intellectual property rights that you hold in that content" (Terms of Service). This clause is necessary otherwise users would not have the confidence to upload their work to Google services such as Google Drive for fear that their intellectual property will be appropriated.

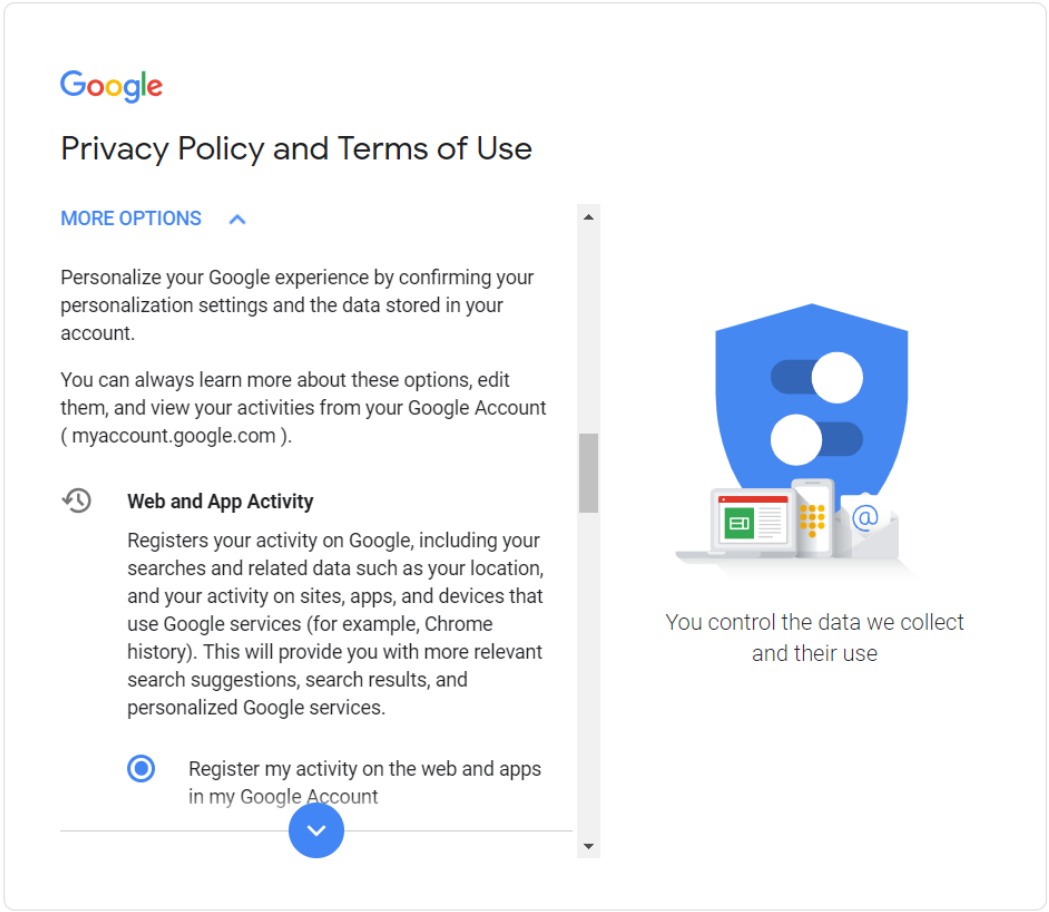
Conclusion

Due to the countless data breaches over the last couple of years, consumers have become acutely interested in what happens with their data. Therefore, laws like GDPR and the California Consumer Privacy Act will continue to be accepted in the future in order to meet the demands of the people. As a result of Google's vague Privacy Policy statements and its lack of transparency, the company does not meet the GDPR regulations and will likely have to accept the sanctions given by the CNIL. In order

to avoid future limiting laws, companies should take the necessary steps for protecting user data to avoid having the public demand the creation of such laws.

Appendix

Pre-checked boxes and need to open “More Options”



Works Cited

AFP. (2019, January 21). *France uses new EU data law to fine Google €50 million.* Retrieved from https://www.thelocal.fr/20190121/france-uses-new-eu-data-law-to-fine-google-50-million

Euronews. (2019, January 21). *France fines Google €50 million using EU's transparency and consent law.* Retrieved from https://www.euronews.com/2019/01/21/france-fines-google-50-million-using-eu-s-transparency-and-consent-law

Fedorenko, S. (2019, January 15). *Amazon Ring faces a data breach scandal as it's blamed for accessing customers' videos.* Retrieved from https://tamebay.com/2019/01/amazon-ring-faces-data-breach-scandal.html

Gaus, A. (2019, January 23). *Alphabet's $57 Million Data Fine: Drop in the Bucket, or Sign of Trouble Ahead?* Retrieved from https://www.thestreet.com/technology/alphabet-s-57-million-data-fine-drop-in-the-bucket-or-sign-of-trouble-ahead-14842470

Intersoft Consulting. (n.d.). *GDPR.* Retrieved from https://gdpr-info.eu/

The Local. (2019, January 21). *Why France hit Google with a whopping €50 million fine.* Retrieved from https://www.thelocal.fr/20190121/why-france-fined-google-50-million

Porter, J. (2019, January 21). *Google fined €50 million for GDPR violation in France.* Retrieved from https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil

Sandal, T. (2018, December 31). *Is Facebook pushing the U.S. closer to a form of EU GDPR?* Retrieved from http://www.digitaljournal.com/internet/is-facebook-pushing-the-usa-closer-to-a-form-of-eu-gdpr/article/539888

Vinocur, N. (2019, January 23). *Google fine launches new era in privacy enforcement*. Retrieved from https://www.politico.eu/article/google-fine-privacy-enforcement-france-gdpr/