Konnor Dickinson
Sihan Xu
John Tran

GDPR and the Right to Be Forgotten

- Discuss circumstances where you think a Right to Be Forgotten is appropriate or provide an argument that a Right to Be Forgotten is never appropriate.

Cases in which Right to be Forgotten is an appropriate rule to follow are cases in which private information or imagery has been posted without the consent of the person whom this information regards; for example, “revenge porn”, or nude images sent privately between couples and then later publicly distributed without the creator’s consent, or private information, such as their home address, phone, number and other related “dox” that could cause harm to that person as a private citizen.

Also, information that is no longer true or relevant and is damaging to a private citizen would be an appropriate case for Right to be Forgotten.

An argument where a Right to Be Forgotten is not as appropriate could be records of fraud and embezzlement of a company’s clients’ funds were misused. There have already been a number of cases like that involving large bank corporations, like Wells Fargo and Bank America, but the point is that kind of activity was hidden for a number of years and threatens the mutual trust of banks (as an intermediary of monetary transactions) in general.

- What are some of the implications of GDPR for you as a developer?

Sihan Xu : Increase the workload of the security team.

Konnor: As a developer of any kind of website, you’d have to be careful about what users are allowed to post, as you, as the host of said site, could get into legal trouble for whatever content is posted there. However, it should be noted: This is *only true* inside of Europe. As citizens of the United States, the implications of the GDPR are much less severe, as any of its fines or consequences would be limited to EU-hosted websites. The GDPR is still relevant to you as a non-EU citizen, but this limitation only exists if your website keeps track of the IPs or records cookies from your customers’ browsers, or if you provide some kind of service to EU customers. In such cases, the GDPR could be very severe, as it will limit how you collect their data and what data of theirs that can be used.

In addition, this brings up the issue that certain pieces of legislation and regimes can affect others on a global scale (as mentioned above with the scope of GDPR). Regardless of our compliances with GDPR, there will inevitably be other laws (maybe even in the near future) that might even overshadow GDPR. As a result, as a developer, we will need to collect personal information of some sort and we can be sure there will be other challenges to overcome (maybe concerning systems that utilize mass amounts of

data--like AI). Another issue could concern surveillance governments (like with China now) where a single individual can't quite be solely responsible for infringement of GDPR.

An obvious reason would be the burden placed on us since trying to handle and maintain code that ensures privacy could be a big hassle (starts even before the design phase).

- Do you agree with the decision in the Google case? Why or why not?

The problem with the Google case, as well as all Right to Be Forgotten cases, is that fundamentally, this can and will be used maliciously and it is naive to assume otherwise. An obvious case of this would be a business manipulating the legal system to force sites to remove true information that negatively impacts said business—such as Amazon removing articles about the mistreatment of their warehouse workers. While privacy is a tremendous issue when dealing with the internet as a whole, litigating what happens on the internet is much easier said than done—if one were to post "revenge" porn of a former partner on, for example, an anonymous imageboard, litigating them in specific will become almost impossible, as it would very quickly become impossible to determine who was the original distributor of said image and who were simply the proxies that were reposting it.

Well, the argument made in "It's Time to Forget the Right to Be Forgotten" does bring up a fair point where in a society that places greater emphasis on blockchain systems, it is sort of a direct conflict of ideas that could prove to be a messy ordeal in hindsight if both were kept as they are right now. As mentioned in the Google article, it does set a precedent on future cases and the gray area where the GDPR of the EU could affect essentially any part of the world (as long as there's some influence on EU people). So, it might have been a lost cause from the start (and how the article above also mentions the inability to enforce such a law).