Off the Grid: The Right to be Forgotten

Dakota LeRoy

Computer Systems Security Final Paper

Abstract

Many web applications claim that once you hit the "delete account" button, all of your data is erased from their servers. However, popular apps such as Tinder have been criticized for maintaining user profiles after deletion in order to boost the number of "active" users. What keeps these companies accountable for wiping user data upon the user's request? Lawmakers in Europe began the attempt to keep search engines accountable for not listing information that citizens request to be removed with a data protection bill, "The Right to be Forgotten." The right to be forgotten is the idea that any user has the right to request that their data be removed from a cyber service at any time, and that the service must comply. In addition to the right to be forgotten, several countries have begun proposals for other data protection legislations. Some of these have a greater scope than monitoring search engines, and current technologies do not currently support their demands. In this paper I will explore a brief history of the European data protection laws that initiated this conversation and the implications of such policy, the feasibility of completely erasing user data upon request, and what services and citizens can do to increase the security of online information they want removed.

Introduction

What happens when you delete something off of the internet? Is it ever really gone? In recent years the European Union has been creating policy to regulate data removal in order to keep commercial services accountable for properly wiping user information. Throughout the early 2010s the EU legal landscape was engrossed in the Google versus Spain controversy. What began as a complaint from citizen Mario Costeja González over publications from 1998 listing

his name resulted in what is known today as the "Right to be Forgotten." This data protection bill began with the 1995 Data Protection Directive and, after the EU's 2014 ruling, was expanded to ensure a person's right to ask for the removal of personal data from a commercial service once it is no longer needed. The policy now specifically targets search engines, stating that information could be maintained on its original website, but would be removed from query results (EPIC, "The Right to Be Forgotten Google vs. Spain"). Thus began a new discussion about our digital footprint and how governments would work to protect citizens on and offline. Although no policies have been created outside of the EU, there have been numerous legal battles in Europe surrounding the bill and formulation of additional legislation. However, the further the law covers citizen's rights, the more apparent it becomes that most services do not have sufficient ways to securely delete data. The juxtaposition of their lack of transparency and governments' desire to increase security of online data creates a technical problem that does not currently have a successful solution.

To the Community

In an article for The Guardian published in August 2017 by Suzan Moore, she writes: "The right to be forgotten is actually about the right to have a past that is not always perfect." The ability to delete references of your data upon request is a powerful tool, and the power to override a user's decision and maintain a reference to their information is even more so. The implications of the bill are far reaching; what about governments with differing policies? For instance, will a user's data still be available on Google Canada if it is being removed from Google Spain? Additionally, some believe being able to go off the grid could create a dangerous

way for people to hide questionable things from their past, or obstruct details or evidence that might play an important role in investigations.

However, even with stringent regulation and widespread cooperation, the ability to entirely wipe a user's data may not be feasible. Despite what services advertise, clicking "Delete Account" will not ensure your information no longer exists or is inaccessible to the highly skilled hacker. Encrypting information and offering more secure database options would help block access to data, but it is ultimately extremely difficult to remove someone's digital trail. Yet billions of devices are connected to the internet, leaving electronic breadcrumbs that are left unswept.

Applications

In 2010 a citizen of Spain used the National Data Protection Agency to make a formal complaint against a local newspaper Google Spain over an article involving personal information he wanted removed. The case was brought forward to the Court of Justice of the European Union and in 2014 they made a ruling. The court stated that if a search engine has a branch in the member state, it must act under EU data protection laws and maintain the right to be forgotten, which the ruling detailed as a citizen's ability to ask a search engine to remove links containing their personal information (European Commission, "Factsheet on the 'Right to be Forgotten' Ruling"). The concept of the right to be forgotten spread beyond the European Court of Justice's ruling with Theresa May's Conservative Party campaign for Prime Minister. She originally ran with the platform of data removal from social media of a any user under the age of eighteen, however she eventually extended it to include any user data from any time. As of August 2017

May's intended legislation would be different from the right to be forgotten; it would also expand personal data to include IP addresses, internet cookies, and DNA. May's proposal reaches further than social media sites and search engines, and services failing to comply with the legislation would be posed with steep fines (Rowena Mason, The Guardian).

Regardless of the scope of these new pieces of legislation, there are some points they do not seem to consider. For instance, it is extremely simple to take screenshots of user's posts on most mobile and web applications. These photos will remain even if that user chooses to remove their account. Although the user's profile, on Facebook for example, will not appear in an internet search such as "Jane Doe Facebook" as it would if the account were active, screenshots of this user's information could still be saved before their account is deactivated and shared later. Additionally, many email providers only remove references to messages upon deletion rather than actually removing them from the database. In an interview with senior staff technologist at the Electronic Frontier Foundation, Jacob Hoffman-Andrews, he said it is "hard to 'completely' delete data because systems like hard drives, databases, applications, and others often mark data as deleted instead of actually wiping it" (Daniel Terdiman, Fast Company). Should the database be compromised, the messages will still be available and exploitable. In order for the right to be forgotten to fully protect a user, the policy would need to deem the provider's current method of deletion as insufficient and require the service to improve its security.

Action Items

Web and mobile applications need to implement higher levels of security because it is currently so difficult to actually delete someone's data. This requires that databases and hard

drives create a secure deletion option, something that is not often prioritized. This is often because many services are reluctant to remove their users as it is advantageous for them to maintain an increasing number of user accounts. Additionally, these services should encrypt all data so that if the information becomes available or is recovered, it will be useless. These actions are necessary for cyber security to match the demands of the data preservation policies and ensure citizens' rights are properly protected.

Governments are creating these laws without fully understanding the nuances of cyber security. As senior threat research advisor at Trend Micro, Paul Ferguson, said in an interview, "...it's a fool's errand to ever expect personal information to be permanently and completely removed" (Daniel Terdiman, Fast Company). Nonetheless, services uphold the illusion that total erasure is possible. Commercial technologies need to be more transparent with data storage and removal procedures in order for lawmakers and citizens to make decisions that advocate for their security online. There is a gap between what is currently implemented in the world of technology and what policy makers expect to be possible in the world of legislation, and it must be bridged. The right to be forgotten is extremely important to uphold, but if services do not fully wipe user data, or even have the means to do so, have we ever actually been privy to it?

Defences

Since the number of internet-connected devices is ever increasing and current technologies do not sufficiently delete user data, there are few ways citizens or governments can truly protect themselves from leaving behind an untraceable digital trail. The most secure way to ensure information is not available online is to never put it there to begin with, but this is often

unrealistic. However, it is possible to make choices about the services one uses in order to minimize the data left behind. For example, avoiding applications that use or capture images of your face, use your fingerprints, or track your location, is a good start. Even with bills like "The Right to be Forgotten," it is often up to the user's own discretion to make decisions that secure their information; the only way to truly go off the grid is to never be on it in the first place.

Conclusion

There have been honorable efforts from European politicians to advocate for citizens' data protection rights, but there is a disconnect between what lawmakers believe is feasible and what is our current internet reality. It is clear that lawmakers want to regulate technology without fully understanding the challenges facing cyber security, and that working solutions to the problem of securely wiping user data are not black and white. The right to be forgotten is a promising start to a future where user's have total control of their online presence. However, developers have a lot more work to do in order to meet these needs. This will require that commercial services change their priorities from maintaining user retention to protecting the rights of their customers. Furthermore, removing online information is not something consumers are requesting yet, but in an age of ever increasing digitization, this will become more of a demand that services must prepare for.

References

Center, Electronic Privacy Information. "EPIC - The Right to Be Forgotten (Google v. Spain)." Electronic Privacy Information Center, epic.org/privacy/right-to-be-forgotten/.

"Factsheet on the "right to be forgotten" ruling." Ec.europa.edu, European Commission, ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

Hern, Alex. "ECJ to rule on whether 'right to be forgotten' can stretch beyond EU." The Guardian, Guardian News and Media, 20 July 2017, www.theguardian.com/technology/2017/jul/20/ecj-ruling-google-right-to-be-forgotten-beyond-eu-france-data-removed.

Manjoo, Farhad. "'Right to Be Forgotten' Online Could Spread." The New York Times, The New York Times, 5 Aug. 2015, www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html.

Mason, Rowena. "UK citizens to get more rights over personal data under new laws." The Guardian, Guardian News and Media, 6 Aug. 2017, www.theguardian.com/technology/2017/aug/07/uk-citizens-to-get-more-rights-over-personal-data-under-new-laws.

Moore, Suzanne. "The right to be forgotten is the right to have an imperfect past | Suzanne Moore." The Guardian, Guardian News and Media, 7 Aug. 2017, www.theguardian.com/commentisfree/2017/aug/07/right-to-be-forgotten-data-protection-bill-ownership-identity-facebook-google.

Terdiman, Daniel. "Why Deleting Personal Information On The Internet Is A Fool's Errand." Fast Company, Fast Company, 22 July 2015, www.fastcompany.com/3048871/why-deleting-personal-information-on-the-internet-is-a-fools-errand.