DATA RETENTION POLICY

Lee Acheampong

School of Cybersecurity

CYSE 525W

Professor Teresa Duvall

1/28/2024

DATA RETENTION POLICY

The cybersecurity policy I have selected is User Data Retention Policy. User data retention deals heavily with how user data is stored and kept by different companies and organizations. Many organizations store user data for a long period as a way to track their user's activities and derive patterns and insights from their data. User data retention policies serve as a way for organizations to classify different types of user data, how long user data can be stored in the organizations' databases and servers, who is responsible for said data, and also what disposal methods are in place for retained user data. I chose this topic specifically because of how user data can be abused by organizations, and leaked by malicious agents, as well as how retained data can still affect individuals long after they've provided this information. Additionally, I will also assess how data retention affects user's right to privacy. Considering the "popularization of the Internet, a great many people conduct electronic communications very frequently, and hence a record of those communications would be extraordinarily intensive and revealing" (Clarke, 2015), so it is of extreme importance that systems are put into place to protect the interest of the people.

An impactful background on user data retention can be derived from the EU's Data Retention Directive. This directive was put in place as a method of combating terrorism and crime. The EU proposed that "following the terrorist bombings in Madrid and London the EU felt a strong need for harmonised rules on communications data retention throughout the

Union," and thus, the Data Retention Directive was born (Svendsen 2007, p. 31). The landscape of the early 2000s instilled fear and panic in the people as well as the government, due to the frequency of terrorist attacks and criminal events. The initial adoption of the Data Retention Directive in "February of 2007" (Svendsen 2007, p. 31) had a profound effect on the citizens of the EU and influenced many data and privacy laws moving forward. The EU's Data Retention Directive outlined a specific set of requirements that was expected of many different phone companies and internet services providers (ISPs) to essentially capture and store data from users. These types of data ranged from " the telephone numbers of callers and those receiving the calls, but also numbers involved in rerouting, names and addresses of subscribers or registered users, and the type of telephone service used. For Internet services, data revealing users' identities (ID) and IP addresses must be retained. Data related to mobile services must also include the international mobile subscriber identity of callers and those receiving the calls (IMSI) and the international mobile equipment identity of both parties (IMEI)" (Svendsen 2007, p. 31-32).

Additionally, the Data Retention Directive imposed a time limit for data that requires "all categories of data covered by the directive must be retained for a minimum of six months and a maximum of two years" (Svendsen 2007, p. 32). Although with this time-imposed time range, there were ways that data could be potentially kept for much longer as "Member States can allow retention periods of more than two years for a limited time, subject to the

Commission's approval," (Svendsen 2007, p. 32). The EU's Data Retention directive eventually fell out of favor with the people as cries of human rights and privacy rights violations were called into account. "In April 2014, the European Court of Justice declared the Data Retention Directive invalid, because it 'exceeded the limits imposed by compliance with the principle of proportionality"(Clarke, 2015). The decision to make this directive invalid by the EU's Court of Justice was a momentous one as it was the first time the courts had made a decision regarding privacy and internet freedom, (CyberGhost VPN, 2014).

With the ever-growing impact of the cloud and cloud security, data retention policies must have requirements for cloud servers as well. According to (Li J. et al 2012), "Data retention belongs to a class of data policies, called *action policies*, that specify what to do (the action) under the current situation" (p.393). This establishes the realm that data retention resides in as a policy. Data retention is heavily influenced by the actions of organizations and companies who have access to these data, and sometimes even government entities. With this policy associated with the actions policies, there must be impactful and effective ways for data retention policies to be carried out. Specifically with cloud security and data retention user data should be treated with the utmost safety for deletion and one method displayed to achieve this is that "each file is associated with a retention policy, and often, permanent deletion of the file at a specified expiration time is an important part of its retention policy. Permanent and secure deletion of files is difficult because files can be replicated in online or offline

environments (for instance, to achieve fault tolerance), and keeping track of the multiple copies is almost impossible. However, if a file is encrypted, then deleting its encryption key is tantamount to permanent deletion of the file and all its backups" (Li J. et al 2012 p.393). This method of data deletion ensures the user data is protected after being utilized by companies to assist users, and limits the ability of this data to be stolen by unauthorized and malicious hackers. Additionally, this method of data deletion prevents organization and company access to the data after it has been deleted, ensuring that there isn't a way to effectively undermine the policy.

Although the new Financial Conduct Authority (FCA) policy on data retention, there seem to be some aspects of this policy that go against the General Data Protection Regulation (GDPR) policy, in many ways a successor to the EU's Data Retention Directive from 2007, that is meant to delete all information on users. In this article, according to Reichman "The FCA points firms in the direction of the Information Commissioner's Office (ICO), which oversees compliance with these rules, and has issued guidance stating firms can refuse to comply with a request for erasure if this is for the "exercise or defence of legal claims"" (Reichman 2018, p. 1). This claim made by Reichman in the article goes on to further explain that " there were ways to 'soft-delete' client files, meaning files were effectively hidden but not deleted and could be recalled when needed" (Reichman 2018, p. 1). With this caveat in place, agencies could still have important data information in place but hide it, which doesn't truly adhere to data

retention policies and methods of deleting user information, but in cases like this this caveat does seem necessary to provide some help when it might be plausible to do so.

The CPRA (California Privacy Rights Act) goes even further than the scope of the GDPR when addressing the importance of user data retention. According to Federman "the law (CPRA) introduced a new definition of sensitive personal information (SPI) that is even broader than the "special categories of personal data" designation under the GDPR. CPRA's SPI definition includes new data types like precise geolocation, genetic data, religious beliefs, biometrics, and health data" (Ferderman 2021 p. 1). Additionally, the article goes on to state "Companies also must offer consumers new options to limit the use and disclosure of their sensitive personal information"(Ferderman 2021 p. 1). This action implemented by the CPRA not only does its absolute best at creating effective policy, as it essentially decreases the amount of information able to be manipulated by companies while also combatting "the growing volume of data in very large databases" (Kalfus et al., 2004).

The landscape of User Data Retention as a policy has increasingly evolved and continues to do so with new mediums of technology as they emerge. These policies not only keep us safe from private entities that would want to use our information against us, but this policy also denies the surveillance of citizens over an extended period. The deletion of user data and safe storage of them is central to having an effective User Data Retention Policy.

REFERENCES

Svendsen, B. (2007). The EU Directive on Data Retention-An End to Justify the Means. *TELEKTRONIKK*, *103*(2), 31.

Reichman. (2018). FCA policy on data retention trumps GDPR deletion rule. *Financial Adviser*, 1.

Federman, Heather. "Exploring the California Privacy Rights Act." Risk Management 12 2020: 10-1. ProQuest. Web. 27 Jan. 2024 .

Clarke. (2015). Data retention as mass surveillance: the need for an evaluative framework. *International Data Privacy Law*, *5*(2), 121–132. https://doi.org/10.1093/idpl/ipu036

Li, J., Singhal, S., Swaminathan, R., & Karp, A. H. (2012). Managing Data Retention Policies at Scale. *IEEE Transactions on Network and Service Management*, *9*(4), 393–406. https://doi.org/10.1109/tnsm.2012.101612.110203

Kalfus, O., Ronen, B., & Spiegler, I. (2004). A selective data retention approach in massive databases. *Omega*, *32*(2), 87–95. https://doi.org/10.1016/j.omega.2003.09.015

Philpotts, M., & 93digital. (2016, September 22). *Improper Data Removal & Poor Enforcement of Data Retention Policies Create the "Perfect Storm" for Data Breaches – Blancco*. Blancco.https://www.blancco.com/improper-data-removal-poor-enforcement-data-retention-policies-create-perfect-storm-data-breaches/

CyberGhost VPN. (2014). Data Retention Directive Declared Invalid in the EU [YouTube Video]. In *YouTube*. https://www.youtube.com/watch?v=iMm-AmiFLh0