Contents

Introduction

This paper will discuss the changes made in the new us-eu Privacy Shield framework. The us-eu Privacy Shield is the replacement for the now defeated Safe Harbour rule. Both Safe Harbour and Privacy Shield aim to protect EU citizens data being stored on servers located in the US. This is only acceptable if the company storing the data can ensure it is complying with the guidelines outlines in the frameworks.

Background

What is Safe Harbour

To understand what Privacy Shield is its important to know where it came from and why it is being used. US-EU Privacy Shield is the replacement for Safe Harbour Privacy Principles most often simply referred to as Safe Harbour. The term Safe Harbour means an agreement that allows protection for liability once certain conditions are met. ("What Is Safe Harbor? Definition and Meaning" n.d.). What this means is that safe harbour is not a law but a guideline that allows companies to act in confidence that they are not breaking any laws in place around the area which they are working in. For the Safe Harbour Privacy Principles outlines a number of principles that US companies could follow to be in compliance with the EU's Data Protection Directive. This allows us

companies like facebook and google to store data that they may have on EU citizens on servers located outside of the EU.

Why is is necessary

Within the Eu there are very strict privacy laws. The Data Protection Directive Provides (*EUR-Lex - 31995L0046 - EN* n.d.) protection to EU citizens regarding the processing of personal data. In the EU citizens data is protected under the Human Rights law. The right to privacy is strongly enforced by all members of the EU. This is much stricter then within the US. This is why the Safe Harbour Privacy Principles was first created. While safe Harbour didn't have any legally binding, It allows US companies to comply with laws from another jurisdiction. The OECD issued seven principles *Notice, Purpose, Consent, Security, Disclosure, Access and Accountability* . ("OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD" n.d.) which the US endorsed but didn't give any fines if they were not followed.

Seven Principles

- **Notice** - People should be to when they data is being collected
- **Purpose** - Should be clear what the data is being used for and not used for any other reasons
- **Consent** - personal data should not be disclosed with the users consent
- **Security** - any data stored should be store securely
- **Disclosure** - people should be informed as to who is collecting their data
- **Access** - people should be allowed access the data and correct any mistakes
- **Accountability** - anyone collecting data must have someone who is held accountable in the event the above rules are not followed

These were not binding as even within the EU there are different privacy laws in each country. This is one of the reasons the Data Protection Directive was created, it helps the free flow of data within the EU.

What did it solve

While Safe Harbour is not perfect it did help the free flow of data between companies that are outside the EU and those within. While people may not think this is a good thing from a privacy point of view. In the current age of cloud computing and SaaS business models it effects more then just users social media data. Workday are a company which have taken advantage are selling

SaaS and advocates of free flowing data as it adds values to there product. Shaughnessy (2017)

> Our position is that national or other jurisdictions' data localization requirements are a well-meaning but ineffective means to ensuring data privacy and security

What was wrong with it

Safe harbour was an agreement which allowed companies to store data from European citizens in servers located outside of the EU. This enabled companies like google and facebook to keep any data they may have on EU citizens in servers located in the US. Under Safe Harbour this was fine as long as where the data was being stored was secure. While Safe Harbour is not a law itself but a regulation that allows the companies that follow it assurances that they are complying with the rules that are in place for data production and privacy for EU citizens. What this meant for companies was that if they followed Safe Harbour they would be comply with the Data Protection Directive

When Edward Snowden leaked documents that showed the US agencies NSA was undertaken a mass surveillance on US citizens. It was a major concern in the Us. The full effect of these leaks may not have been fully realised in Europe until later. These leaks showed how the CSI and NSA were spying on data on an indiscriminate basis by access servers which could have had both US and EU citizens data. This is a violation on EU rights and in turn makes Safe Harbour void as companies can't ensure data is not being used for its indented purpose. While this is quiet clearly a big problem it wouldn't be until Max Schrems brought a case to the European Court of Justice that we would see the fallout of the Snowden leaks.

Max Schrems

Max Schrems is an Austrian lawyer who while studying abroad for a semester was writing a paper about Facebook Privacy issues. He discovered what he taught was flaw in the safe harbour framework after the Snowden leaks. Where the NSA and access to a backdoor to facebook and other websites which were storing EU citizens data in there US servers under Safe Harbour. He first filed a complaint to facebook Ireland Ltd with the Irish Data Protection Commissioner as Ireland in the country where Facebooks EU Headquarters are located. This case was thrown out for be 'frivolous'. (*Reuters* Wed Oct 07 17:04:29 UTC 2015) Billy Hawks Data Protection Commissioner said that the companies had nothing to answer for. Mr.Hawks continued by saying "if you're not doing anything out of the way, you should not expect to have your data accessed." ("Hawkes to Take No Action Against Apple, Facebook" 2013) Not to be defeated, Schrems

continued with his case against facebook to the European Court of Justice. Arguing that privacy should not be something won in court. Saying "I want my things should stay private should not be a topic, because it's a basic right. The same way that I don't have to argue why I want the right to vote". (*Reuters* Wed Oct 07 17:04:29 UTC 2015) He was successful in saying that EU citizens data should not be transfers to countries where there are lower privacy standards then in the EU. In 2005 the ruling came back to say that the safe harbour framework was invalid. ("EU-US Data Sharing Deal Not Valid, ECJ Rules in Irish Facebook/Max Schrems Case" n.d.) This meant that a new framework had to be created to help with the free flow of data.

Privacy Shield

Privacy Shield is the new framework that the will replace safe harbour. It came on the 12th of July in 2016. Its goal is to enable the free flow on data between the EU and US companies. As the US laws don't provide an adequate level of protection, this new framework ensures that the data in being stored securely.

Similar to Safe Harbour the Seven Principles still apply ("Bryan Cave - Privacy Shield Finalized - How Everyone Can Take Advantage of the New European Data Transfer Framework" n.d.) of *Notice, Purpose, Consent, Security, Disclosure, Access and Accountability* . Unlike Safe Harbour compiles must include statement on each principle to state how they are going to implement each principle. To compile with Privacy Shield compiles must annually self-certify. This process will be unchanged from safe harbour but will be more actively monitored by the Department of Commerce. They plan on doing this with questionnaires. The FTC are going to keep track of companies that don't meet compliance with a "Wall of Shame" of companies that have court orders in Privacy Shield cases. ("Five Ways That Privacy Shield Is Different from Safe Harbor and Five Simple Steps Companies Can Take to Prepare for Certification" n.d.) For EU citizens that think there data is being miss handled, they can now report this to there local Data Protection Authorities. For Ireland this simply involves writing to the Data Protection Commissioner with the details of the issue and the organisation. ("Making a Complaint to the Data Protection Commissioner - Data Protection Commissioner - Ireland" n.d.) While Privacy Shield hasn't been without criticism, with some saying it doesn't do enough to protect EU citizens or give them enough rights to challenge companies in court which they believe may be misusing their data. Irwin (2017) Schrems himself thinks that the Us Government still has to much access to get this information.

Conclusions

Its very easy to think that the Privacy Shield is something that just effects average people and how there data is being shared within companies. This is a framework after all that came about from a court case against facebook sharing with the US government it aid in a mass surveillance program. While nobody wants to have there data being shared without there knowledge its probably native to think that we can use these social media services and get to keep our privacy. I agree with Max Schrems and think that EU personal data should not be accessed by the US government for any form of surveillance. However we need to understand that this also has huge effect of businesses that are trying to do create something of value. Instead of making framework perfect we should be more actively getting changes to it so that in the yearly review it gets updated and becomes more effective for protecting EU citizens. You will never make a prefect framework for such a complex issue such as privacy law between countries however making something that can be changed quickly and adapt as new technologies come out is something that could be achieved.

References

"Bryan Cave - Privacy Shield Finalized - How Everyone Can Take Advantage of the New European Data Transfer Framework." n.d. Accessed February 18, 2018. https://www.bryancave.com/en/thought-leadership/privacy-shield-finalized-how-everyone-can-take-advantage-of-the.html.

"EU-US Data Sharing Deal Not Valid, ECJ Rules in Irish Facebook/Max Schrems Case." n.d. Independent.ie. Accessed February 20, 2018. https://www.independent.ie/business/technology/euus-data-sharing-deal-not-valid-ecj-rules-in-irish-facebookmax-schrems-case-31551267.html.

EUR-Lex - 31995L0046 - EN. n.d. Accessed February 18, 2018. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046.

"Five Ways That Privacy Shield Is Different from Safe Harbor and Five Simple Steps Companies Can Take to Prepare for Certification." n.d. Accessed February 19, 2018. https://www.paulhastings.com/publications-items/details/?id=eaffe969-2334-6428-811c-ff00004cbded.

"Hawkes to Take No Action Against Apple, Facebook." 2013. *RTE.ie*, July. https://www.rte.ie/news/2013/0726/464770-data-protection/.

Irwin, Luke. 2017. "Privacy Shield Passes Yearly Review Despite Mounting Criticism." IT Governance Blog. October 2, 2017. https://www.itgovernance.eu/blog/en/privacy-shield-passes-yearly-review-despite-mounting-criticism/.

"Making a Complaint to the Data Protection Commissioner - Data Protection Commissioner - Ireland." n.d. Accessed February 19, 2018. https:

//www.dataprotection.ie/docs/Making-a-Complaint-to-the-Data-Protection-Commissioner/r/18.htm#How%20do%20I%20make%20a%20complaint?

"OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD." n.d. Accessed February 18, 2018. http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Reuters. Wed Oct 07 17:04:29 UTC 2015. "Max Schrems: The Law Student Who Took on Facebook," Wed Oct 07 17:04:29 UTC 2015. https://www.reuters.com/article/us-eu-ireland-privacy-schrems/max-schrems-the-law-student-who-took-on-facebook-idUSKCN0S124020151007.

Reuters. Wed Oct 07 17:04:29 UTC 2015. "Max Schrems: The Law Student Who Took on Facebook," Wed Oct 07 17:04:29 UTC 2015. https://www.reuters.com/article/us-eu-ireland-privacy-schrems/max-schrems-the-law-student-who-took-on-facebook-idUSKCN0S124020151007.

Shaughnessy, Jim. 2017. "Why Workday Advocates the Free Flow of Data Throughout the EU." Workday Blog. June 12, 2017. https://blogs.workday.com/why-workday-advocates-the-free-flow-of-data-throughout-the-eu/.

"What Is Safe Harbor? Definition and Meaning." n.d. BusinessDictionary.com. Accessed February 18, 2018. http://www.businessdictionary.com/definition/safe-harbor.html.