EU-US Cloud Privacy Crash

• Why • How • What's Next •

Author: Dan Shearer

First Published: 25 October 2017

Last Update: 15 November 2017

Sponsored by Kopano

Table of contents

Abstract

US companies' legal right to supply internet cloud services to EU citizens or EU companies is questionable and under intense pressure. EU privacy laws are much stricter than US laws, and temporary fixes to bridge the gap are not looking credible. Two new EU privacy laws (the GDPR and the ePrivacy Directive) are based on privacy as a human right for EU citizens or residents worldwide, where in contrast, the US approach is to remove privacy protections from non-US citizens, even when US companies are operating in Europe.

Services developed to be compatible with the US market tend to be incompatible with the GDPR and ePrivacy. An EU company can easily detune from EU standards to US standards if required to do business in the US, within certain limitations. Unfortunately for US companies, doing things the other way around is very difficult and expensive, and in the prevailing legislative environment, there's a notable chance that it is not possible at all. This means that EU businesses have a significant advantage. It is possible though for a US cloud provider to become fully GDPR compliant, but this has no value without Privacy Shield or some alternative.

Privacy Shield however, has all but collapsed. This special arrangement is about US companies self-certifying that they will treat personal data of EU citizens according to EU law. The US government, US courts and the President of the US have now made decisions which ignore even the best intentions of US cloud companies. In the EU, several bodies are now close to deciding whether the Privacy Shield will continue or cease to exist. Without Privacy Shield or a proper alternative, US cloud companies cannot legally supply services to EU companies or citizens.

Overview

US companies' legal right to supply internet cloud services to EU citizens or EU companies is questionable and under intense pressure.

EU privacy laws are much stricter than US laws, and temporary fixes to bridge the gap are not looking credible. As American companies, they must ultimately obey US law, not EU law. There is overwhelming evidence suggesting that EU personal data is not safe with a company whose headquarters is in the US. Pitted against this are increasingly thin promises that there will be a functional solution reconciling the EU and US systems at some point in the future.

But what does this mean, practically? Fortunately, we do have some answers:

- **There is no disaster scenario.** Planned change and migration is needed but that is normal in the cloud business. No instant shutdowns of US companies will happen and alternatives exist.
- **Privacy is economically significant.** The EU has made privacy and online trust the starting point for the European Digital Market. This is not just about checkboxes.
- **Human rights are economically significant.** The EU is enforcing online privacy as a human right, with many related rights. This builds on 65 years of European human rights experience creating a predictable environment for markets to develop.

Privacy is the immediate major force for change and the topic of this paper, but as important background, there is also the more slow-burning matter of competition. Both privacy and competition issues are about US companies behaving as if they are above the law of any country. The EU has taken very strong action against these companies in 2017 for abusing their dominant position, including billions of euros in fines - and more is expected before 2018.

About This Document

This is a factual description for business and technical purposes of:

- The collapse of privacy agreements between the US and EU over a period of years accelerated by recent court cases and actions on both sides of the Atlantic.
- The details of why Privacy Shield is collapsing, and what is happening right now.
- The EU's Single Digital Market vision leading to the GDPR and the ePrivacy Directive.
- Some discussion of the GDPR and the ePrivacy Directive.
- The need for EU-controllable and EU-based replacements to US cloud services.

To discuss these matters these are also covered: basics of relevant laws, some highlights from history and the expressed intentions of the EU and US institutions.

Introduction

This document seeks to support the following advice to EU companies and citizens:

Move to EU-based cloud or self-hosted products, because of the proven risk to personal data and changes in law and technology. Don't wait for slow fixes and legal arguments.

The facts are clear. Like coal-burning power stations or financial behemoths, these US companies seem too big to fail or to be replaced by anything. However, there are quality European alternatives that do not have the multiple risks of US-sourced cloud products.

The reason for the statement is that the EU and the US are incompatible on privacy:

Two new EU privacy laws (the GDPR and the ePrivacy Directive) are based on ***privacy as a human right*** *for all people worldwide, where in contrast, the US approach is to* ***remove privacy protections from non-US citizens****, even when US companies are operating in Europe.*

There are many things happening in parallel. But now in September 2017, this is the big one:

The special arrangement called ***Privacy Shield is being widely challenged.*** *Privacy Shield is about US companies self-certifying that they will treat personal data of EU citizens according to EU law. However, the US government, US courts and the President of the US have made decisions which ignore even the best intentions of US cloud companies. In the EU, several bodies are close to making decisions.*

"The special arrangement called Privacy Shield is being widely challenged."

US cloud companies have dominated the Western world, and while there are EU-based alternatives they have a much smaller mindshare. Businesses and people in the EU need help to understand statements such as *"You need to find alternatives to Google Apps, Amazon Web Services, Rackspace Hosting and Microsoft Office365.*

The privacy debate surrounding the processing of EU data by US companies is affected by many factors and incidents and reactions. ***However, these factors are either predominantly or all negative.*** That is why the risk profile of US cloud providers continues to increase.

What Will Happen For Sure?

In this paper full references are given for the following:

- The GDPR will become enforceable in May 2018.
- The draft ePrivacy Directive will become law and enforceable soon, probably in May 2018.
- The EU Parliament will vote on the validity Privacy Shield in 2017 after the Commission's September 2017 review.
- The EU General Court will issue a decision on Privacy Shield in 2017 or 2018.
- The EU Commission is considering further major 2017 fines for anti-competitive behaviour.
- The US Supreme Court decided in October that it will review the US Government's claim that it can order US companies to supply EU data, see the section 'Update: Status as of November 2017'
- The US Supreme Court will decide by October if it will review the US government's extraterritorial powers. Can US courts order US companies to supply EU customer data?

We can also be relatively sure that the large US cloud companies and the EU Commission will continue their understated panic about the doubt surrounding Privacy Shield, while at the same time telling customers "nothing will change, we are big, global providers and your data is safe with us."

We can also be relatively sure that the American NSA and the UK's MI5 will continue to gather data indiscriminately on a huge scale, activity which is strictly illegal under the GDPR and proposed ePrivacy Directive, and that the US administration of President Trump will continue to be hostile to both the idea of privacy in general and respecting the rights of non-US citizens.

"We can be relatively sure that the American NSA and the UK's MI5 will continue to gather data indiscriminately on a huge scale. "

What *Might* Happen?

Changes in the legal and technology environment cannot be predicted. But there are some things that are possible, perhaps even probable:

- Privacy Shield might well be struck down, by an EU court, the EU parliament, or even (however reluctantly) by the EU Commission, whose relevant Commissioner is reviewing Privacy Shield in September 2017. There is a lot of evidence, cited in this paper, of the many interest groups that want this to happen. The US and other governments are, by their actions, very worried that this might happen. The EU Commission is has a need to acknowledge both camps.
- Fines for GDPR non-compliance may be issued by the existing national privacy bodies from May 2018. These could be very substantial.
- Technologies such as encryption, peer to peer, IPv6, and blockchain may become increasingly adopted since they make GDPR and ePrivacy compliance easier and better.
- Technologies such as cloud search might well become much less popular. That is certainly what Google and many other companies seem to think will happen.
- EU cloud software providers might find it much easier to get their marketing message out if US cloud providers can no longer say that they are equal to EU providers.
- US President Donald Trump might drive even more privacy-unfriendly activities by the US government, which would accelerate concerns in the EU about how US companies will be either allowed or forced to behave inappropriately.
- New investment in EU-based cloud solutions may well happen if the market appears to be getting more competitive via privacy issues, competition issues, or other things.

"Technologies such as encryption, peer to peer, IPv6, and blockchain may become increasingly adopted since they make GDPR and ePrivacy compliance easier and better."

What is the History?

This is a story of two different paths. The US has, since before the year 2000, been decreasing protections of non-US citizens from the activities of US companies, and ever-increasing intrusion by the NSA and other US organisations. The EU has, over the same period, decided to base its economic future around giving its citizens reason to trust online markets, and has focused that trust on strict controls on handling personal data. These two things are totally in conflict.

"This is not just a narrative of two totally incompatible worldviews, because the EU and the US are connected on many levels, as are other regions of the world. "

Within the last 18 months events discussed in this document have created irresistible pressures for change:

- Certain US and EU court cases
- Actions by the current US administration with respect to non-US citizens
- Actions by some US companies in the EU and the US
- Actions by some US government agencies taking the data of non-US citizens
- The EU GDPR legislation was passed
- The ePrivacy Directive was approved in draft form

This is not just a narrative of two totally incompatible worldviews, because the EU and the US are connected on many levels, as are other regions of the world. For example, despite the increasing gap on privacy, Europe very nearly signed the TTIP trade agreement which would have subjected EU citizens to US commercial rules, similarly to the Canadian CETA agreement[1].

1. https://www.tni.org/en/publication/making-sense-of-ceta-2nd-edition. The parts of CETA over which the EU has exclusive control are in force from September 2017, however, each member state still has to ratify provisions such as the highly controversial commercial court system.

Despite the EU agreeing to it, CETA had to be renegotiated after the European Court of Justice ruled that its data transfer rules were illegal[2]. The EU is therefore not being combatively independent, just consistently strong on protecting privacy in ***real actual fact***. The EU is also composed of institutions that have very different points of view, in particular, the Commission has often prioritised the smooth running of the existing EU economy over improved principles for the future. The Commission is the most susceptible to pressure from US industry and its EU subsidiaries.

"For a pragmatic response to the facts in the EU today, there is, unfortunately, only one consistent answer - don't use US clouds. "

For a pragmatic response to the facts in the EU today, there is, unfortunately, only one consistent answer - **don't use US clouds.** It is possible that things will get better for US companies, but it will take years.

2. https://www.privateinternetaccess.com/blog/2017/07/transatlantic-data-flows-renewed-threat-following-top-eu-courts-ruling/ Last week, Europe's highest court issued what might seem a fairly obscure ruling on an agreement between the EU and Canada on the transfer of passenger data between the two regions. In fact, the implications of the judgment by the Court of Justice of the European Union (CJEU) are far reaching, and are likely to have a major impact on the flow of all personal data across the Atlantic.

Limiting the Scope of This Document

Privacy issues and legislation are complex and there are many kinds of cloud-based services, too many to cover effectively in this paper.

This document is limited to the kinds of cloud services where EU citizens regularly make changes to their stored data, such as Facebook, Google Apps/Gmail, and Twitter. It also covers the case where EU companies use US providers for hosting entire applications, such as Amazon Web Services, Microsoft Azure or Softlayer. There are EU-sourced and EU-based equivalents for all of these products.

Privacy data law also applies to many other kinds of cloud services which are out of scope for this document, including search and online shopping, hybrid mobile services, and more. It is significant that even Google appears to have recognised that technology changes are making search obsolete, and the things replacing search have very different privacy considerations.

Little mention is made of Model Contracts (or Standard Contractual Clauses) as an alternative mechanism to Privacy Shield. This mechanism overlaps in its enforcement with Privacy Shield and is addressed in the Update: November 2017 section.

The Right Rights: Declaration,Charter, Convention

The UN's famous 1948 Universal Declaration of Human Rights[3] is the ultimate ancestor for many legally binding documents both at the UN level and in many countries, and it includes a section on privacy. The 47 countries in the Council of Europe[4] ratified one such document, created in 1953. Of these 47 countries, the 27 in the European Union ratified a more specific and updated document in 2009.

"The UN's famous 1948 Universal Declaration of Human Rights is the ultimate ancestor for many legally binding documents both at the UN level and in many countries, and it includes a section on privacy."

When considering the GDPR and the proposed ePrivacy Regulation, it can be easy to confuse two human rights documents:

1. The 1953 European Convention on Human Rights is an evolving document derived from the Universal Declaration of Human Rights. For 65 years the Convention, together with the history of decisions made by the EU Court of Human Rights, has been the basis for human rights law in Europe and beyond. The Convention is enforced within the 47 member states by the European Court of Human Rights in Strasbourg, which is a specialist court just for Human Rights matters.
2. The 2009 European Charter of Fundamental Human Rights[5] is exclusively a document for European member states, unlike the Convention. The Charter is enforced within the 27 member states by the Court of Justice of the European Union[6] (CJEU) in Luxembourg, which is for any EU matter. Within the CJEU are the Court of Justice and the General Court (both of which are relevant to understanding Privacy Shield in 2017.)

3. http://www.un.org/en/universal-declaration-human-rights/index.html The Universal Declaration of Human Rights

4. http://www.coe.int/en/web/portal/home The name "Council of Europe" is easy to confuse with be confused with the Council of the European Union or the European Council, both of which are part of the EU governing apparatus. The Council of Europe has nothing to do with any European Union institution. It is an international organisation aiming to "uphold human rights, democracy and rule of law" in Europe and to promote European culture. With 47 members including Turkey and Russia this is a broad view of what "European" means.

5. http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm The Charter of Fundamental Rights of the EU brings together in a single document the fundamental rights protected in the EU. The Charter contains rights and freedoms under six titles: Dignity, Freedoms, Equality, Solidarity, Citizens' Rights, and Justice.

6. https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en Court of Justice of the European Union (CJEU) Ensures EU law is interpreted and applied the same in every EU country and that countries and EU institutions abide by EU law.

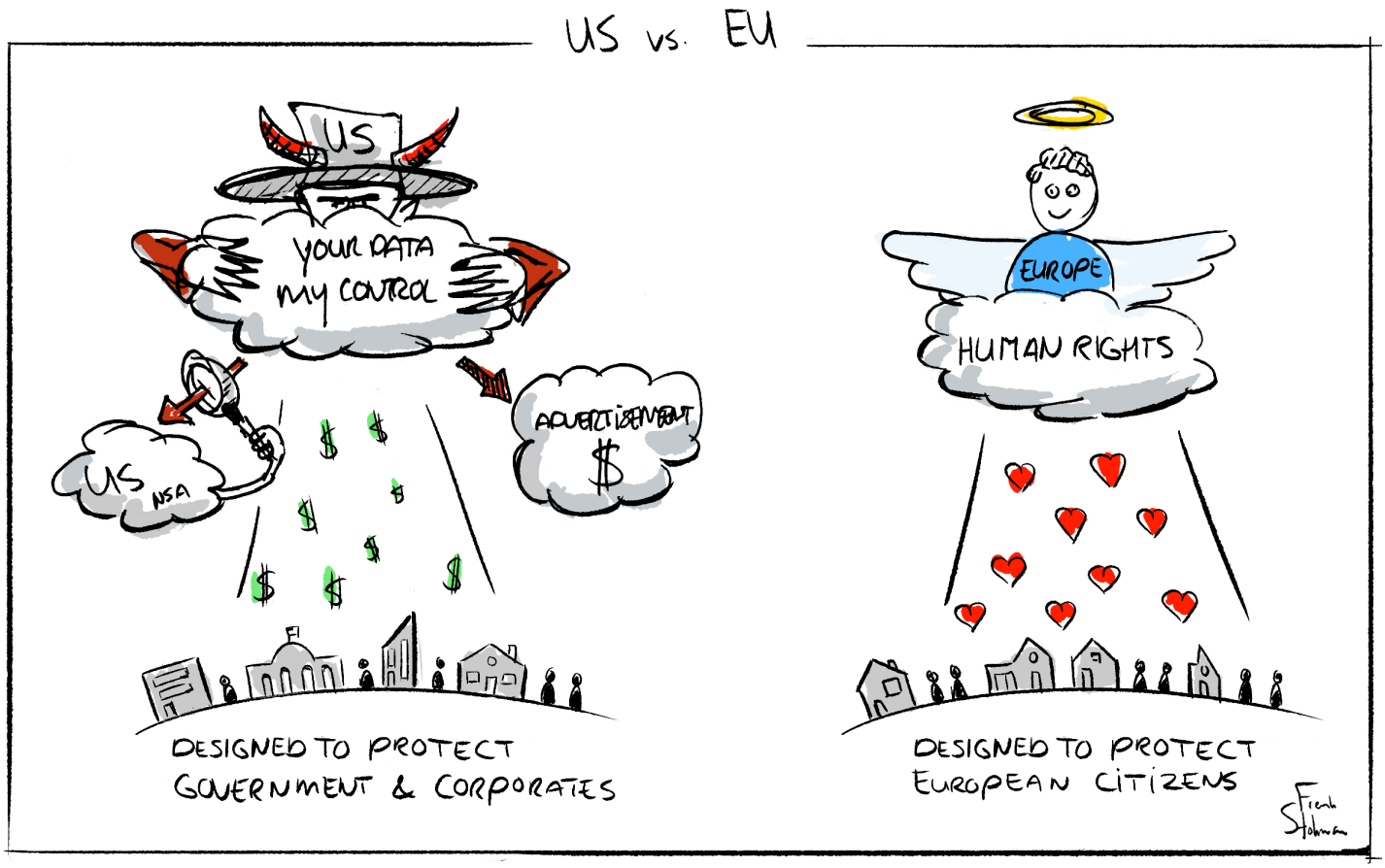
Part of the confusion between the Convention and the Charter happens when referring to Article numbers because the numbers do not match up. The GDPR and ePrivacy regulation were drafted after 2009, so they refer exclusively to the Charter. This document does not refer to Convention Articles from this point on.

"The Charter is not a brand new document, more of an extension of the Convention. "

The Charter is not a brand new document, more of an extension of the Convention. The Charter says in Article 52 that it is 100% compatible with the Convention, but the Charter may go beyond:

... the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.

Examples of the Charter exceeding the Convention in scope are where it includes social rights and principles relating to the workplace and some things that the Convention is too old to have included, such as cloning of tissue or data privacy rights.



At the beginning of the GDPR the Recitals[7] mention five human rights from the Charter besides those core to the GDPR and ePrivacy, here with the Charter Article numbers inserted:

This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications [Article 7], the protection of personal data [Article 8], freedom of thought, conscience and religion [Article 10], freedom of expression and information [Article 11], freedom to conduct a business [Article 16], the right to an effective remedy and to a fair trial [Article 47], and cultural, religious and linguistic diversity [Article 22].

Since the Charter has only come into effect in 2009, most of the information that exists on examining these fundamental rights and freedoms is based on the Convention. One of the first major cases to explore the balance between public and private data since the Charter came into force was Google Inc vs Agencia Espanola de Proteccion de Datos, discussed in the section **Privacy in Europe Under the 2009 Charter**.

"One of the first major cases to explore the balance between public and private data since the Charter came into force was Google Inc vs Agencia Espanola de Proteccion de Datos"

7. https://gdpr-info.eu/recitals/ "Considering the following reasons the articles of the GDPR have been adopted. These are the latest and final recitals of April 27th 2016."

Key Factors & Players

The following programmes, documents and institutions are referred to throughout this document.

The Digital Single Market

The key EU policy driving the entire question is an economic one: The Digital Single Market [8]. This is a project at least a decade old aiming to increase the amount of trade conducted within the EU by electronic means, and to ensure that the *"EU economy, industry and employment take full advantage of what digitalisation offers."*

The Digital Single Market strategy continues:

"... existing barriers online mean citizens miss out on goods and services, internet companies and start-ups have their horizons limited, and businesses and governments cannot fully benefit from digital tools. It's time to make the EU's single market fit for the digital age – tearing down regulatory walls and moving from 28 national markets to a single one. This could contribute €415 billion per year to our economy and create hundreds of thousands of new jobs."

Under this Strategy, the Commission has a Policy called "Strengthening Trust and Security" [9] which says:

"The European Commission's initiatives aim to improve online security, trust and inclusion. Trust and security are at the core of the Digital Single Market Strategy."

"The European Commission's initiatives aim to improve online security, trust and inclusion. Trust and security are at the core of the Digital Single Market Strategy."

8. https://ec.europa.eu/commission/priorities/digital-single-market_en "Digital Single Market: Bringing down barriers to unlock online opportunities."i

9. https://ec.europa.eu/digital-single-market/en/policies/strengthening-trust-and-security Policy document under the Single Digital Market Strategy.

The logic is that without trust, there will not be universal adoption and without universal adoption, the Digital Single Market will fall short. Online privacy initiatives including legislation are all part of building trust, and also part of protecting all fundamental rights online, not just privacy.

"The logic is that without trust, there will not be universal adoption and without universal adoption, the Digital Single Market will fall short."

Legal Documents

There are three essential legal instruments:

- Privacy Shield[10] (2016)
- GDPR[11] (2016, with enforcement from May 2018)
- Draft ePrivacy[12] Regulation (hoped to be passed, and take effect May 2018)

There are three other legal instruments which have recently become essential to understand why Privacy Shield continues to exist at all:

- Presidential Order for Enhancing Public Safety in the Interior of the US [13] (January 2017)
- EU-US Umbrella Agreement[14] (cited in the immediate worries about the Presidential Order)
- US Judicial Redress Act[15] (the legal underpinning of The Umbrella Agreement)

10. https://www.privacyshield.gov/EU-US-Framework Download the full text of the EU-US Privacy Shield and Annexes.
11. https://gdpr-info.eu/ A neatly arranged English PDF version of the General Data Protection Regulation (GDPR) including its recitals.
12. https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications Download the PDF titled "Proposal for a Regulation of the European Parliament and of the Council"
13. https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united Stripping non-US citizens of privacy protections is part of the intention to "Make use of all available systems and resources to ensure the efficient and faithful execution of the immigration laws of the United States;"
14. http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf "Protection of Personal Information Relating to Prevention, Investigation, Detection and Prosecution of Criminal Offenses."
15. https://www.congress.gov/bill/114th-congress/house-bill/1428 H. R. 1428 "This bill authorizes the Department of Justice (DOJ) to designate foreign countries or regional economic integration organizations whose natural citizens may bring civil actions under the Privacy Act of 1974 against certain U.S. government agencies for purposes of accessing, amending, or redressing unlawful disclosures of records transferred from a foreign country to the United States to prevent, investigate, detect, or prosecute criminal offenses."

Institutions & Structures

The situation around Privacy Shield is not understandable without knowing a little of the institutions and structures involved, including the competing and conflicting interests.

"The situation around Privacy Shield is not understandable without knowing a little of the institutions and structures involved."

The following are referred to in this document (with some of their most notable activities):

European Union:

- European Commission (certified Privacy Shield as "Adequate" in July 2016)
- European Parliament (asked Commission to fix Privacy Shield in April 2017)
    - LIBE Committee (Listed Privacy Shield deficiencies, March 2017)
    - Article 29 Working Party (asked Commission to fix P.S. June 2017)
- Court of Justice in the EU
    - European Court of Justice (struck down predecessor to P.S. October 2015)
    - General Court (reviewing the P.S. Adequacy decision, 2016-2017)

United States:

- Supreme Court (numerous decisions against privacy rights for non-US citizens)
- Presidency of Donald Trump (has acted several times to reduce privacy)

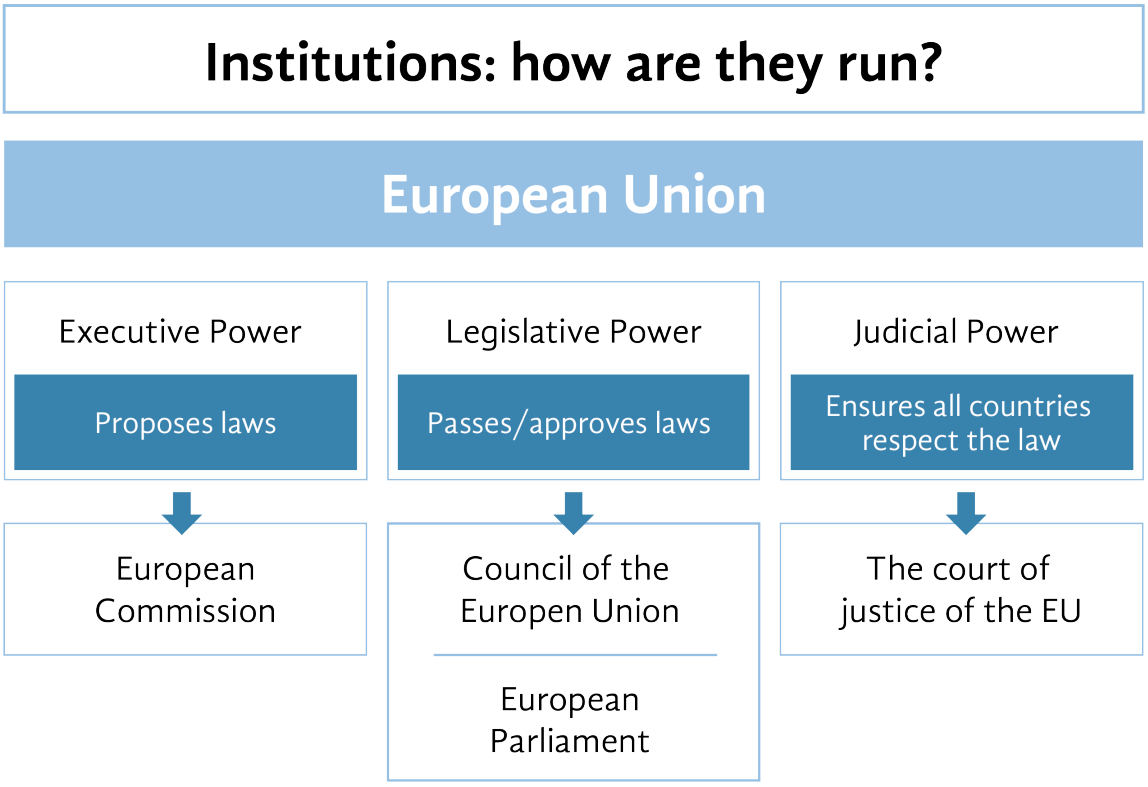


Fig. 1. How EU institutions work

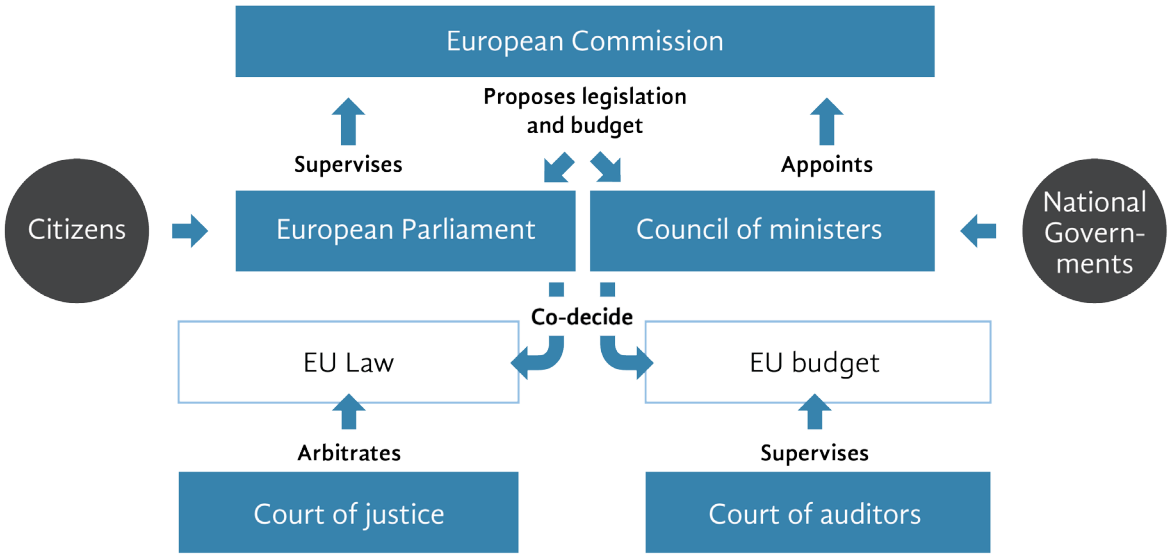


Fig. 2. Workflow EU institutions

The Council of Ministers in figure 1 is now called the Council of the European Union (not to be confused with the European Council or the Council of Europe, which are unrelated but very significant organisations in their own right.)

Key Argument

Key Argument Part 1

While the GDPR and ePrivacy are crucial to this argument, ***the key thing about US clouds in Europe is Privacy Shield, not how good or bad the US cloud companies are in terms of the GDPR and ePrivacy.*** If Privacy Shield is held to be inadequate (as it the not-yet-binding view of many, detailed in the section Privacy Shield as at 22nd September 2017) then US cloud companies cannot legally supply services to EU companies or citizens.

Key Argument Part 2

In addition, the GDPR and ePrivacy are vital to the way any EU cloud replacement is implemented. Services developed to be compatible with the US market tend to be incompatible with the GDPR and ePrivacy. In the US, for example, a company has the right to comprehensively spy on its employees and US-based cloud software supports this[16]. In the EU such rights are greatly restricted, and EU-based cloud software should be designed from the beginning to support this. This conflict is highlighted in the words of the GDPR about "Data Protection by Design and Default"[17].

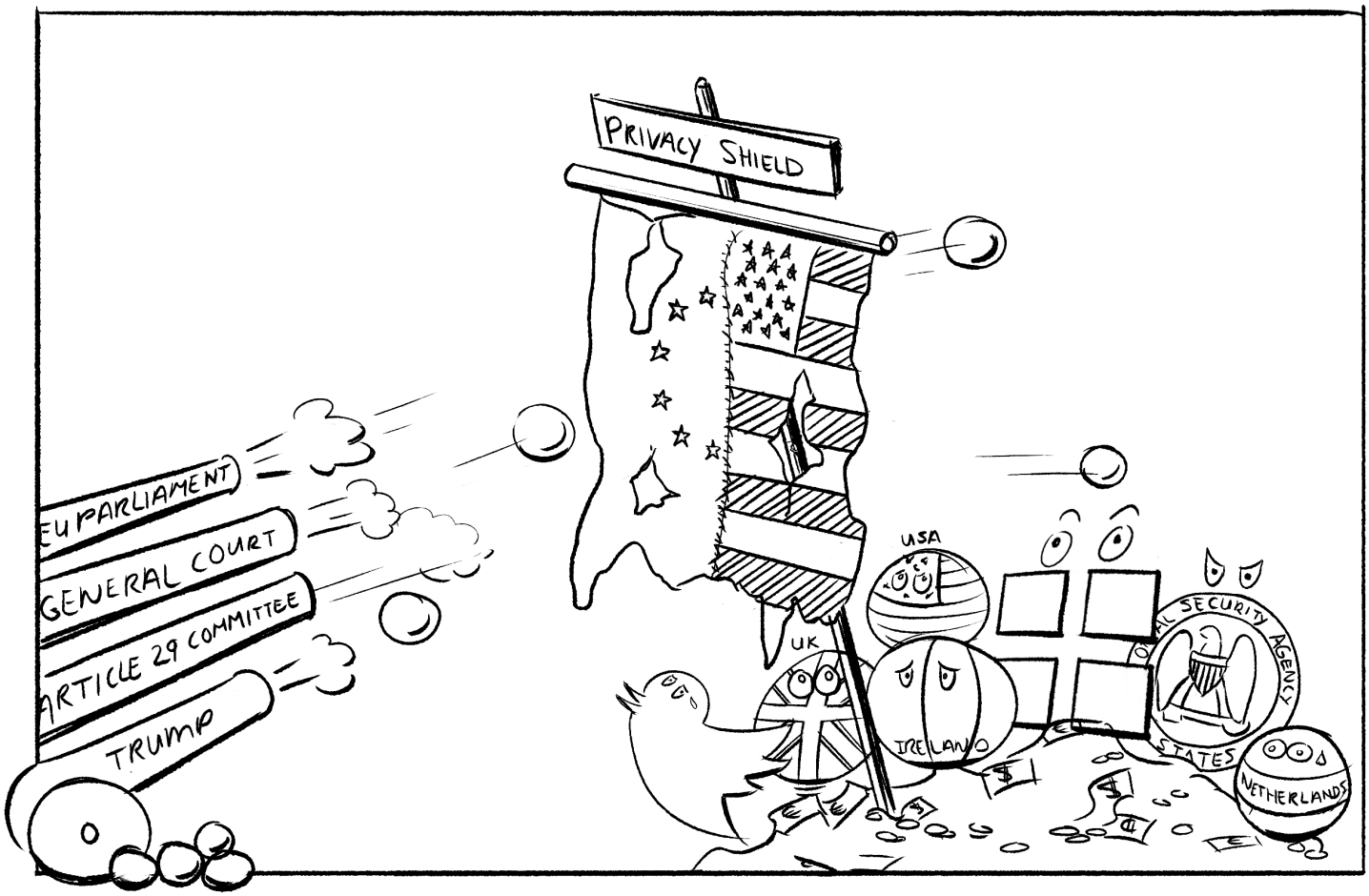
There is no reason why a US cloud provider cannot implement good privacy. It is possible for a US cloud provider to become fully GDPR compliant, but that has no value without either Privacy Shield continuing or some alternative.

"It is possible for a US cloud provider to become fully GDPR compliant, but that has no value without either Privacy Shield continuing or some alternative."

16. https://www.americanbar.org/content/dam/aba/events/labor_law/2016/04/tech/papers/monitoring_ella.authcheckdam.pdf "It is well established that whatever an employee sends or receives on a company email account is the property of the employer and can be accessed or viewed by the company without notice." and "Many employees are discovering, however, that messages sent on private accounts can also be accessed under certain circumstances if they use a company-issued computer, smart phone or tablet. Former General and CIA Director David Patraeus even had his Gmail account accessed by the FBI." These are two examples of behaviour that is legal in the US but generally illegal under EU law.

17. https://gdpr-info.eu/art-25-gdpr/ This is often misquoted as "Privacy by default", a phrase that does not exist in the GDPR.

Privacy Shield



Privacy Shield is a 2016 self-certification scheme for US companies to hold themselves to the strict privacy rules of the European Union when processing data related to EU entities. Article I says:

In order to rely on the Privacy Shield to effectuate transfers of personal data from the EU, an organization must self-certify its adherence to the Principles to the Department of Commerce (or its designee) ("the Department"). While decisions by organizations to thus enter the Privacy Shield are entirely voluntary, effective compliance is compulsory: organizations that self-certify to the Department and publicly declare their commitment to adhere to the Principles must comply fully with the Principles.

The European Parliament oversees Privacy Shield via the Article 29 Working Party . They published an FAQ . (Note: The Article 29 Working Party will soon be replaced by the European Data

18. https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg Full Text of the Privacy Shield

19. http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 Working Party on the Protection of Individuals with Regard to the Processing of Personal Data.

20. http://ec.europa.eu/newsroom/document.cfm?doc_id=40943 EU-US Privacy Shield F.A.Q for European Individuals

Protection Board, which will oversee the GDPR and have more power than the Article 29 Working Party.)

On Friday 22nd September 2017 the US appointed[21] Lisa Sotto as arbitrator for Privacy Shield. It is noteworthy that not until the end of the week in which Privacy Shield had its first annual review, did the US appoint the arbitrator required for Privacy Shield to function.

The status of Privacy Shield is unknown, pending the review of the United States' enforcement procedures and other aspects. There has been very little positive to say from the EU side, particularly given the Trump administration's actions relating to privacy and implementation of Privacy Shield.

History of Privacy Shield

Privacy Shield was created in 2015 following the Schrems v Data Protection Commissioner[22] court case where the EU Court of Justice was mostly persuaded by evidence of the NSA spying on EU citizen's personal data[23]. Quick political decisions were made, and the Commission published its Privacy Shield Adequacy Decision[24] in July 2016. It is clear from the text that the Decision is a hastily constructed document, including letters of promise from US officials and letters of demand from EU officials. Nevertheless, it has legally binding effect because it was approved by the EU parliament, albeit for a limited time only, subject to very strict review, and generally with little trust.

"It is clear from the text that the Decision is a hastily constructed document, including letters of promise from US officials and letters of demand from EU officials.."

21. https://www.huntonprivacyblog.com/2017/09/22/lisa-sotto-selected-as-arbitrator-for-the-eu-u-s-privacy-shield/ Lisa Sotto Selected as Arbitrator for the EU-U.S. Privacy Shield

22. https://epic.org/privacy/intl/schrems/ "Two of the most important international privacy cases in recent history arose from complaints against Facebook brought to the Irish Data Protection Commissioner by an Austrian privacy advocate named Max Schrems."

23. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362 "Judgment of the Court (Grand Chamber) of 6 October 2015. Maximillian Schrems v Data Protection Commissioner."

24. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016D1250&from=EN "COMMISSION IMPLEMENTING DECISION (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield"

The adequacy decision, and with it Privacy Shield, came into effect from 1st August 2016[25].

Privacy Shield immediately came under intense criticism:

- March 2017 - The EU Parliaments Civil Liberties Committee passed a resolution about deficiencies[26]
- April 2017 - An EU Parliament Resolution was passed asking the Commission to remedy deficiencies[27]
- June 2017 - Article 29 Working Party sent a letter citing deficiencies to the EU Commision[28]

This was no surprise. The previous version of Privacy Shield was Safe Harbour[29] and its provisions were under serious criticism, with the EU Parliament Resolution of March 2014[30] identifying at least five occasions since 2000 where the Parliament or Commission had highlighted problems on the US side for delivering appropriate privacy protections.

25. https://en.wikipedia.org/wiki/EU-US_Privacy_Shield
26. http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/RE/2017/01-12/1111803EN.pdf This document is very strongly worded in it's suspicion of Privacy Shield. It "Stresses that... Deplores that... Regrets... Regets... Calls on... Instructs..."
27. http://www.europarl.europa.eu/news/en/press-room/20170329IPR69067/data-privacy-shield-meps-alarmed-at-undermining-of-privacy-safeguards-in-the-us "New rules allowing the US National Security Agency (NSA) to share private data with other US agencies without court oversight, recent revelations about surveillance activities by a US electronic communications service provider and vacancies on US oversight bodies are among the concerns raised by MEPs in a resolution passed on Thursday."
28. http://ec.europa.eu/newsroom/document.cfm?doc_id=45272 "Preparation of the Privacy Shield Annual Joint Review ... the Art. 29 Working Party (WP29) issued several opinions and stressed that its concerns would have to be addressed within the framework of the annual EU/US Joint Review of the Privacy Shield. The first joint annual review will be therefore a key moment for the WP 29 to assess the robustness and effectiveness of the Privacy Shield mechanism."
29. https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles "The Safe Harbor Privacy Principles were developed between 1998 and 2000 in order to prevent private organizations within the European Union or United States which store customer data from accidentally disclosing or losing personal information. They were overturned on October 6, 2015 by the European Court of Justice (ECJ)... "
30. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230

The thing that finally caused the end of Safe Harbor was the publication of Edward Snowden papers in 2013[31], which was the major reason cited by the European Court of Justice in striking down Safe Harbor[32]. There is no need in this paper to go into the history of Safe Harbor, only that this is just the beginning of the evidence that Safe Harbor was an attempted fix to two incompatible approaches to privacy, and Privacy Shield an even quicker fix when Safe Harbor proved inadequate.

Of the many criticisms of the Privacy Shield by the Article 29 Working Party is that the US administration of President Trump has not put the mechanisms in place to enforce it. As explained in the Article 29 Working Party's FAQ the intention is:

"Of the many criticisms of the Privacy Shield by the Article 29 Working Party is that the US administration of President Trump has not put the mechanisms in place to enforce it."

Where the informal panel of EU Data Protection Authorities (DPAs) is not competent, EU DPAs have the possibility to refer the complaint to US authorities (notably, the FTC committed to giving priority consideration to those referrals and the Department of Commerce has a clear deadline to act on complaints). In many cases, depending on the circumstances of the case, the competent national DPA may also directly exercise its powers (such as prohibition or suspension of data transfers) toward the EU data exporter.

On the US side, enforcement relies in part on the Privacy and Civil Liberties Oversight Board, which has, in effect, ceased activities in the administration of President Donald Trump[33], since it has as of September 2017 only one single board member remaining[34].

31. https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present) Documents US government policies and actions disregarding the privacy of non-US citizens and international agreements signed by the US Government regarding handling of personal data.
32. https://techcrunch.com/2015/10/06/europes-top-court-strikes-down-safe-harbor-data-transfer-agreement-with-u-s/ Natasha Lomas "the European Court of Justice has today declared invalid the Safe Harbor data-transfer agreement that has governed EU data flows across the Atlantic for some fifteen years."
33. http://www.politico.com/agenda/story/2017/01/privacy-board-trump-national-security-000264 This article is about an oversight agency intended for internal US concerns, but the Privacy Shield agreement extended that to EU matters.
34. https://www.pclob.gov/about-us/board.html as at September 2017 lists only Elisabeth B. Collins as a board member, and there seems no trace of activity by her or statements relating to her role on the committee or its relation to EU privacy matters

Enforcement also relies on the appointment of an Ombudsperson, which is currently an unfilled position. Techcrunch managed to get a statement in April 2017 to the effect that there is a temporary ombudsperson[35]:

"Enforcement also relies on the appointment of an Ombudsperson, which is currently an unfilled position."

Acting Assistant Secretary Garber was delegated the authorities of the Under Secretary for Economic Growth, Energy and the Environment (which includes those of the Ombudsperson under the EU-US Privacy Shield), pursuant to Delegation of Authority No. 415, dated January 18, 2017", and "can exercise those authorities until a new Under Secretary is in place, or until the delegation is revoked by competent authority".

Techcrunch concluded:

So it would appear that the position of Under Secretary for Economic Growth, Energy and the Environment — and therefore the Privacy Shield ombudsperson — remains vacant at this point in the Trump administration's tenure, with only an acting civil servant in place for now.

But that is not the whole story. The entire concept of an ombudsperson as defined in Privacy Shield was brought into question by the European Ombudsman, who wrote an opinion to say that the position as described cannot be sufficiently independent[36] to even qualify for the name "ombudsman":

Article 8 of the EU Charter identifies the essential elements of the fundamental right to the protection of one's personal data and, in its third paragraph, stipulates that "[c]ompliance with these rules shall be subject to control by an independent authority."

... and ...

"Finally, despite the fact that the Ombudsperson will be functionally independent from the US intelligence community, the Department of State, within which it will operate, is an executive department responsible for US foreign policy.

35. https://techcrunch.com/2017/04/06/eu-us-privacy-shield-remains-precariously-placed/ by Natasha Lomas "it could take just a single stroke of Trump's pen to bring the entire [Privacy Shield] arrangement toppling down."
36. https://www.ombudsman.europa.eu/en/cases/correspondence.faces/en/66926/html.bookmark "Follow-up reply from the European Ombudsman to Commissioner Jourová on the use of the title 'Ombudsperson' in the EU-US Privacy Shield agreement."

This department makes use of intelligence provided by the US intelligence community. Given that fact and the Ombudsperson's obligation to report to the Secretary of State, it could be argued that this does not provide for the necessary distance from the intelligence community that is required for the body to act in an independent manner."

The factual situation as at September 2017 is that if there is a privacy complaint raised from the EU to the US by an EU citizen, that there is nobody to hear it, nobody to decide on the complaint, and even if there was, no guarantee that the decision would be fair and independent.

See Also...

This paper does not try to provide an exhaustive legal analysis of Privacy Shield, but others have done that. A comprehensive and useful index to relevant case law, precedent and informed opinion was published[37] in June 2016 by Dena Dernavoic as a Masters Thesis at Lund University.

In July 2017, Human Rights Watch and Amnesty International published a concise and intensely fact-based briefing[38] asking the Commission to reverse its adequacy decision, arguing in part:

Commission should take account of the fact that US officials may use an idiosyncratic definition of "collect" ... we understand this to mean that the [US] government often considers communications to have been "collected" only if an analyst has examined them or otherwise processed them in some way. It follows that the government likely considers it may acquire vast stores of digital information without running afoul of the already limited safeguards against arbitrary "collection" of such information in US law, widening the considerable gap between US practice and the standards set out by the CJEU.

"In July 2017, Human Rights Watch and Amnesty International published a concise and intensely fact-based briefing38 asking the Commission to reverse its adequacy decision,"

37. https://lup.lub.lu.se/student-papers/search/publication/8879990 Safe Harbor No More: Impact of the Schrems Case on EU – US Personal Data Transfers . "The Schrems case marks a pivotal moment in the definition of the notion of privacy and data protection in many ways, among which the downfall of Safe Harbor is the most notable one. Finally, the thesis aims to provide a concise overview of the EU – U.S. Privacy Shield. All of this is looked at through the fundamental rights lens of the EU Charter."

38. https://www.hrw.org/news/2017/07/26/joint-letter-european-commission-eu-us-privacy-shield "Assessment of the Adequacy of US Surveillance Laws and Practices for the Purposes of EU Law"

Since this is exactly the fact as confirmed in many ways since Snowden, Human Rights Watch would appear to be asking the obvious of the Commission. However, there are intense political and commercial pressures on the Commission to do what it can to keep Privacy Shield in place.

"there are intense political and commercial pressures on the Commission to do what it can to keep Privacy Shield in place."

As has been noted above are many other grounds for challenging Privacy Shield than national security overreach, however, it is this issue that finished Safe Harbor and it appears still to be unresolved.

Administration of Donald Trump

The "America First" view of president Trump is well-known, as is his view of "Enterprise First". This has led to a significant erosion of privacy rights in the US in the last year. One significant example is the repeal of privacy for broadband users[39]. When it comes to EU-US privacy, there was a great deal of activity triggered by the Presidential Executive Order Enhancing the Public Safety[40] in January 2017, where Article 14 states:

Sec. 14. Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.

This can seem like it removes privacy protections from EU citizens, and therefore to destroy Privacy Shield immediately. That was the initial reaction by many expert observers, including Jan Philip Albrecht[41] [42] , the leading MEP on privacy.

39. https://www.reuters.com/article/us-usa-internet-trump/trump-signs-repeal-of-u-s-broadband-privacy-rules-idUSKBN1752PR "U.S. President Donald Trump on Monday signed a repeal of Obama-era broadband privacy rules, the White House said, a victory for internet service providers and a blow to privacy advocates."

40. https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united Executive Order: Enhancing Public Security in the Interior of the United States.

41. http://www.europarl.europa.eu/meps/en/96736/JAN+PHILIPP_ALBRECHT_home.html. Note his chairship of the influential Civil Liberties Justice and Home Affairs committee.

42. https://en.wikipedia.org/wiki/Jan_Philipp_Albrecht

He tweeted[43]:

If this is true @EU_Commission has to immediately suspend #PrivacyShield & sanction the US for breaking EU-US umbrella agreement. #CPDP2017

The European Commission reacted urgently within hours[44] stating:

We are aware of the executive order on public safety. The US Privacy Act has never offered data protection rights to Europeans.

The Commission's point is that Privacy Shield has protection and enforcement from the US which is outside the US Privacy Act (although, the enforcement does not appear to exist as of September 2017.) Secondly, the Commission refers to the EU-US Umbrella Agreement, which concerns exchange of data for law enforcement purposes (e.g. anti-terrorism) and to make the Umbrella Agreement effective, Congress passed the Judicial Redress Act.

"In the view of the Commission, the validity of Privacy Shield rests on an act passed by US Congress to facilitate data sharing in the special case data sharing for law enforcement, which is without the consent of the data subject."

Therefore, in the view of the Commission, the validity of Privacy Shield rests on an act passed by US Congress to facilitate data sharing in the special case data sharing for law enforcement, which is without the consent of the data subject.

Nevertheless, even the EU Commission, which has been trying very hard to maintain firstly Safe Harbor and then Privacy Shield, and which has asked to have the court case against Privacy Shield dismissed in the EU General Court – even the EU Commission is not very positive.

43. https://twitter.com/JanAlbrecht/status/824553962678390784 "Trump's Executive Order on 'public safety' directs all federal agencies to exclude non-citizens and LPRs from #PrivacyAct protections.

44. https://www.theregister.co.uk/2017/01/26/trump_blows_up_transatlantic_privacy_shield/ This may be the only source for the alleged statement by the Commission currently findable on the internet, however it does appear to be accepted by authorities as a legitimate quotation.

Věra Jourová[45] the Commissioner for Justice, Consumers and Gender Equality, represents the Commission on Privacy Shield. She said in Parliament in April 2017[46] on the subject of the review now taking place in 2017:

Let me make this point very clear: If we are faced with any developments that could negatively affect the level of protection afforded under the Privacy Shield, the Commission will take its responsibilities and use all available mechanisms – review, suspension, revocation, repeal – to react.

The statement by the Commissioner is both strong (stating willingness to revoke or repeal) and somewhat in denial because as abundantly documented there are already circumstances that would seem to "negatively affect the protections afforded under the Privacy Shield".

This, combined with the general attitude of the current US administration to non-US citizens, and the continued activities of the NSA and other organisations specifically mentioned as invalidating the Safe Harbor arrangement, has led to the current situation of grave doubt about Privacy Shield having any effect at all. While not yet definitively invalid, it is easy to see why there are so many concerns on the EU side at the moment. The direction of travel from this US administration is not promising for Privacy Shield.

"The direction of travel from this US administration is not promising for Privacy Shield."

45. https://ec.europa.eu/commission/commissioners/2014-2019/jourova_en Her responsibilities include "Concluding negotiations with the United States on a data protection agreement to protect the privacy of EU citizens wherever they live."

46. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BCRE%2B20170405%2BITEM-019%2BDOC%2BXML%2BV0%2F%2FEN&language=EN&query=INTERV&detail=3-922-000 5th April 2017, Strasbourg, Adequacy of the protection afforded by the EU-US privacy Shield (debate)

Update: Status as of November 2017

The pace is certainly heating up. On the 16th October, the US Supreme court accepted the case of United States v. Microsoft Corp.,[47] which is about emails stored on a server in Ireland. This is a mirror image of the identical case which brought down Safe Harbor, only in this case being decided in the United States with a very different view of the interests of non-US citizens. Two days later, the European Commission published the results of its review of Privacy Shield[48], in which it was extremely positive about even small advances that it could identify in the practices of the US government, but even this positivism could not hide the work that is needed to fulfill the ten recommendations.

One of the most extraordinary lacks was the fact that no ombudsperson is in place, meaning that to date US companies have been entirely policing themselves, completely avoiding the intent of the GDPR. This is the same US ombudsperson that was supposed to be overseeing data transfers happening outside Privacy Shield under a mechanism called "standard contractual clauses" as explained by the European Commission[49]. This mechanism is also under serious threat since on 3rd October the Irish High Court referred the matter of Facebook data transfers to the EU Court of Justice, saying it "concurred with the Irish Data Protection Commissioner's view there are "well-founded" grounds for believing the European Commission decisions approving data transfer channels known as Standard Contractual Clauses are invalid."[50]

"One of the most extraordinary lacks was the fact that no ombudsperson is in place."

47. https://www.irishtimes.com/business/technology/microsoft-ireland-faces-a-data-privacy-battle-in-us-supreme-court-1.3275201
48. http://europa.eu/rapid/press-release_MEMO-17-3967_en.htm
49. http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf Guide to the EU-US Privacy Shield,
50. https://www.independent.ie/irish-news/courts/high-court-asks-european-court-of-justice-to-examine-facebook-data-transfer-case-36192379.html

These are complex questions:

- Will the US Supreme Court rule in favour of the Trump Administration or EU citizens?
- Will the EUCJ rule in favour of Facebook or EU citizens' rights, in a virtual repeat of the Safe Harbour hearing?
- Will the EU Commission's report on Privacy Shield as "adequate but needing improvements" be accepted by the EU Parliament and its committees?

If Privacy Shield survives all three challenges there are still multiple other actions underway. It is not an exaggeration to say that Privacy Shield is under even more extreme pressure now than it has ever been. For an agreement created in a great hurry composed of letters of intent and promises, perhaps it is surprising it has survived this far at all.

About the GDPR and ePrivacy Directives

Simplistically, the GDPR can be thought of as regulating personal data at rest, and ePrivacy covering personal data when in motion, and other communications. The process of two people communicating by any electronic means involves many steps and a lot of data, and between them, these two instruments try to cover all these steps and possibilities of sensitive data.

"Simplistically, the GDPR can be thought of as regulating personal data at rest, and ePrivacy covering personal data when in motion, and other communications. "

There is a great deal of basic information about the GDPR and ePrivacy Directive[47] on the internet. Here we give a quick overview and then focus on aspects of the legislation relevant to whether or not US cloud companies will continue to dominate the European market. The next section explains why understanding this relationship between the GDPR and ePrivacy is essential to grasping competitive opportunities.

GDPR vs ePrivacy

Broadly speaking, the GDPR is about personal data wherever it is found, and ePrivacy about electronic communications – which may or may not be related to personal data. It is convenient to think of the GDPR as derived from Article 8 of the Charter ("Everyone has the right to the protection of personal data concerning him or her") and ePrivacy from Article 7 ("Everyone has the right to respect for his or her private and family life, home and communications").

"It is convenient to think of the GDPR as derived from Article 8 of the Charter and ePrivacy from Article 7."

There is also a precise relationship between the two, with ePrivacy being lex specialis to the GDPR[51]. Lex specialis means that on some issues ePrivacy expands on what the GDPR says, and if there is a difference, then ePrivacy wins. In addition, according to ePrivacy recitals, ePrivacy will never weaken protections available to individuals under the GDPR[52]. One extremely significant difference is the question who these protections cover. The GDPR explicitly only addresses natural persons, meaning that (unlike in the US) a company cannot claim a right to protection of personal data in the GDPR sense. However, ePrivacy says in Recital 5.3:

Electronic communications data may also reveal information concerning legal entities, such as business secrets or other sensitive information that has economic value. Therefore, the provisions of this Regulation should apply to both natural and legal persons. Furthermore, this Regulation should ensure that provisions of the [GDPR...] also apply to end-users who are legal persons. This includes the definition of consent ... When reference is made to consent by an end-user, including legal persons, this definition should apply. In addition, legal persons should have the same rights as end-users that are natural persons regarding the supervisory authorities; furthermore, supervisory authorities under this Regulation should also be responsible for monitoring the application of this Regulation regarding legal persons.

51. http://data.consilium.europa.eu/doc/document/ST-5358-2017-INIT/en/pdf "This proposal is lex specialis to the GDPR and will particularise and complement it..."

52. ePrivacy Recital 5.5: "This Regulation therefore does not lower the level of protection enjoyed by natural persons under [the GDPR]"

This illustrates the interesting effect of splitting out Charter Article 8 Data Protection (GDPR) from Charter Article 7 Right to a Private Life (ePrivacy). When it comes to data a corporation is not intended to have anything that even looks like an inalienable human right. Not in the EU.

The creation of the GDPR was an intense collaborative (and combative) process. That focus has now moved on to the draft ePrivacy directive. Since ePrivacy is not yet finished, and given the lex specialis relationship, that means there is some fluidity about how the GDPR will work in the future until a final draft of ePrivacy is agreed. That is not unreasonable or unexpected with new legislation, for example there is also fluidity about how GDPR enforcement will work in practice, and what the courts will think of various provisions. Nevertheless, for EU-based mobile and cloud companies, this is very interesting time as an entire sector gets redefined in public, and at very high speed compared to most legislative processes.

GDPR

The GDPR protects the personal data of EU residents when processed by organisations, no matter what organisation or where that organisation is located. The GDPR gives individuals more control over their own personal data, and harmonises rules across the EU, intending to "enhance data protection rights of individuals and to improve business opportunities by facilitating the free flow of personal data in the digital single market"[53].

"The GDPR protects the personal data of EU residents when processed by organisations, no matter what organisation or where that organisation is located."

The GDPR addresses transparency and consent (consent is an important competitive point, more on that later); data portability; expanded rights for the individual; strong emphasis on provable good practice; and very significant potential penalties.

53. http://europa.eu/rapid/press-release_MEMO-17-3191_en.htm A framework for the free flow of non-personal data in the EU

ePrivacy

Technology developments have confused the definitions of what the word "communications" means, so the ePrivacy Directive includes tracking, mobile devices, Internet of Things, software updates, end-to-end encryption, online directory services and more as well as voice communications, email and messaging of all kinds, and any data related to the transmission of electronic communications. There is a strong desire to outlaw even the possibility of backdoors, be they by means of encryption or otherwise. "Take it or leave it" consent clauses will be banned, where a telecommunications provider will be forced to accept customers even if those customers do not wish to permit tracking or other invasive activities.

"ePrivacy is an ambitious attempt to address the huge scope of technology in the 21st century as it applies to individuals, in a world where individual interests and rights are usually bypassed en masse and often by accident."

As an indication of the intensity of the debate, the EU Parliament's Policy Department for Citizens' Rights and Constitutional Affairs commissioned a May 2017 report[53] An assessment of the Commission's Proposal on Privacy and Electronic Communications" which has very detailed criticisms, many of which have been addressed in debate since.

There are ongoing battles between commercial, human rights, technical and legal interests and more. However, the intentions are clear and will not change. ePrivacy is an ambitious attempt to address the huge scope of technology in the 21st century as it applies to individuals, in a world where individual interests and rights are usually bypassed en masse and often by accident. The EU is well aware that large parts of European society are now affected quickly by the use of technology, often technology that is operated according to the worldview of non-Europeans. Since ePrivacy covers all electronic communications, this is a substantial first step is defining how our future world will look like.

54. http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583152/IPOL_STU(2017)583152_EN.pdf May 2017 "The study assesses whether the [ePrivacy] proposal would ensure that the right to the protection of personal data, the right to respect for private life and communications, and related rights enjoy a high standard of protection. The study also highlights the proposal's potential benefits and drawbacks more generally.

Future Potential Points to Consider

Consent – it may seem counter-intuitive, but there is a bias in the effect of the GDPR toward reducing the consent asked of individuals before processing their personal data. The quality of GDPR consent is high, and it can be withdrawn at any time by the data subject. However, there are other valid grounds to process personal data without asking the individual, including a somewhat vaguely worded "legitimate interest" - that is, the legitimate interest of the company processing the data. That might have been the end of the matter, except that ePrivacy also addresses the concept of consent. ePrivacy gives very limited opportunity for a service provider to avoid consent, and yet it inherits the tough consent requirements of the GDPR.

Possible Direction of Travel – This suggests that any electronic processing in the EU will tend to be subject to a particularly European idea of informed consent, which could well have a ripple effect around the world.

Anonymity, and Third Parties – at the same time as the EU Parliament has been debating a perceived need to ensure that electronic cryptocurrencies are not anonymous on anti-terrorism grounds, the GDPR and ePrivacy together are arguably best fulfilled by technologies that have degrees of inherent anonymity. Full anonymity is currently difficult (Monero, Zcash, Tor, and various peer-to-peer, blockchain and torrent-type technologies.) Similarly, anonymity is difficult when there is any kind of third party involved, whether it be an SSL certificate authority or even a directory service such as DNS.

"The GDPR and ePrivacy together are arguably best fulfilled by technologies that have degrees of inherent anonymity."

*Possible Direction of Travel – T*his suggests that anonymity in Europe is back as a legitimate option at the highest levels. Since the GDPR/ePrivacy trend is to disallow the idea of backdoors and third parties, the media companies and state security services can no longer get away with demonising particular technologies. The same may well not be true in the US.

Race to the Top

The entire problem of the EU-US Privacy Shield is that this is a race to the top. The EU has much higher standards in privacy than the US.

An EU company can easily detune from EU standards to US standards if required to do business in the US, within certain limitations. It is definitely easy from a technical point of view if systems have been designed with this in mind.

Unfortunately for US companies, doing things the other way around is very difficult and expensive, and in the prevailing legislative environment there's a high chance that it is not possible at all. Therefore, EU businesses have a very significant advantage.

One Route to Certainty in 2018

Businesses need to make firm decisions around cloud services, and these decisions have significant lead times. Three of the most influential institutions in the world The EU Court of Justice, the US Supreme Court, and the European Parliament are expected to make decisions which may or may not agree with each other, and even very large companies are unable to influence what these decisions will be. As of November 2017, the best we can say is that answers to the biggest Privacy Shield questions will be known during the latter half of 2018. This is a very challenging degree of uncertainty.

Businesses have three choices:

- wait until some point in 2018 before making their decisions as to cloud services, generally meaning rollouts will be no sooner than 2019. This assumes no further challenges to Privacy Shield arise in 2018.
- assume Privacy Shield will exist in 2019 and assume US cloud companies will effectively implement its requirements and that the ombudsperson is an effective mechanism (because if it is not, then Privacy Shield becomes under threat again.)
- adopt EU cloud service provision and therefore meet GDPR obligations directly, meaning Privacy Shield is irrelevant to them, and rollouts can happen in 2018. This is the only way to have certainty in 2018. This certainty needs to be balanced against technical risk.

Users with existing substantial investment in US cloud applications might reasonably decide to wait and see before committing to potentially risky change. For others moving to the cloud for the first time, the biggest risk is likely to be the delay caused by Privacy Shield uncertainty, which is where EU cloud providers have a decisive advantage today. Users of EU cloud need never consider the status of Privacy Shield or other mechanisms, nor be concerned about lawsuits being raised that might impact their cloud software. Users need to decide what their risk appetite is, and anyone relying on US cloud applications in 2018 will inevitably be exposed to uncertainty and perhaps large-scale change forced from the outside.

About Dan Shearer

Originally from Australia via the US and as of 2005 based in Edinburgh, Scotland, I am pleased to be part of the Open Source industry in the UK. I was co-founder of the Samba team and have been involved in many open source projects since.

I'm a consultant and offer services to large businesses in four roles:

- Technologist, dealing with how chunks of technical functionality interact
- Open Source Software specialist, deployment and development
- Product Marketer, refining products for computing, defence and high-tech markets
- Virtualisation specialist, bringing mainframe approaches to business computing

I have worked with many companies from Cable and Wireless Optus, Hewlett-Packard, Fujitsu-Siemens ICL and Westpac Bank through to large government and quasi-government bodies. I'm currently CTO of Privasee, experts in privacy and GDPR compliance. I also enjoy growing small companies to service these big ones with interesting new products, and have worked in several startup operations in three different countries.

dan@shearer.org