Brussels,
19 January 2016,

Dear Chair,
Dear members of the Article 29 Data Protection Working Party Subgroup on the Future of Privacy,

We would like to thank you very much for the opportunity given to Access Now and European Digital Rights (EDRi) to discuss the consequences of the European Union Court of Justice (CJEU) ruling in the case C-362/14 *Maximillian Schrems* v *Data Protection Commissioner* (known as "the Schrems case") on international transfers of personal data.

EDRi is an association of 31 digital civil rights organisations registered or with offices in Council of Europe Member States. We focus primarily on privacy and freedom of communication in the digital age, particularly with regard to issues such as data protection, online law enforcement, and the role of internet intermediaries.

Access Now is an international organisation that works to defend and extend digital rights of users globally. Through representation in 10 countries around the world – including presence in the European Union - Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. Access Now wields an action-focused global community of nearly half a million users from over 185 countries, and also operates a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world.

This document was prepared with the support and contributions from Emeritus Professor of International Law, Douwe Korff.

The Safe Harbour

On 6 October 2015, the CJEU found the Safe Harbour mechanism to be invalid.[1] EDRi and Access Now welcomed this landmark decision which confirmed that the Safe Harbour mechanism is beyond repair, and put an end to over a decade of privacy violations.[2] [3] Safe Harbour was a transatlantic data transfer mechanism enabling companies to send data processed in the European Union (EU) to the United States (US). The framework was established in 2000 to help navigate the differences in how data protection is regulated on either side of the Atlantic. The arrangement was, by its very nature as a self-certified mechanism that lacks oversight and fails to provide meaningful redress, unsafe. Negotiations of this arrangement in the EU were conducted at the sole discretion of the European Commission, which, faced with growing political and time pressure, chose to ignore the privacy concerns raised by civil society groups and the European Parliament.

Case law emanating from the Safe Harbour judgment

The CJEU ruling established that, when personal data are transferred from the EU to the US, the protections should be "essentially equivalent" to those in the EU. The Court found that such equivalence was not achieved by the Safe Harbour, for the following reasons:

1. Under specific US surveillance programmes, US agencies are granted "generalised" – effectively unlimited and indiscriminate – access to personal data such as the content of communications.[4] This impinges on the very essence of the right to privacy as protected by the EU Charter of Fundamental Rights and fails the necessity and proportionality test.

2. Furthermore, there is, in US law, an almost complete absence of judicial remedies for persons whose data are protected by EU law. This impinges on the very essence of the right to an effective remedy encompassed under the EU Charter and can therefore never be justified.

3. The European Commission had tried, by means of the Safe Harbour, to deprive the data protection authorities of the Member States of their independent right and duty to assess the adequacy (now, "essential equivalence") of the law in a third country, contrary to fundamental EU principles.

---

[1] CJEU, Case C- 362/14 Maximillian Schrems v Data Protection Commissioner
http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30ddeee34ab986084cf0ae66808c885c771b.e34KaxiLc3qMb40Rch0SaxuSax10?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1203114

[2] Access Now, CJEU declares Safe Harbour invalid
https://www.accessnow.org/cjeu-declares-safe-harbour-invalid/

[3] EDRi, Fifteen years late, Safe Harbor hits the rocks
https://edri.org/safeharbor-the-end/

[4] See section on the US context below.

4. And crucially, by its very nature, a self-certifying scheme like the Safe Harbour, could not prevent the US companies that adhered to that framework from being forced to provide access to the data covered by the Safe Harbour when requested by US authorities, despite the lack of judicial remedy for data subjects.

We detail below how the fundamental defects in US law still persist, and indeed in some ways have been made worse. We also note that the judicial remedies envisaged in the EU-US Umbrella Agreement - that has been signed but not yet ratified by the EU - does not provide for judicial remedies for persons protected under EU data protection law and the EU Charter who are not EU citizens.[5] [6] As a result, the legal service of the European Parliament has just now come to the unavoidable conclusion that this defect also impinges on the essence of the right to an effective remedy.

In sum, any successor to the invalid Safe Harbour can only be compatible with the EU Charter if it protects all persons protected by the Charter, which mean not only all EU citizens, but also all EU resident, from "generalised", indiscriminate access to their data by US authorities, including US national security agencies. Any new agreement must provides for effective judicial remedies in this respect for all such persons. This means that any new scheme can never be solely reliant on self-certification mechanisms which have failed to provide "adequate" protection for EU fundamental rights.

The US context

In adopting the ruling, the Court has provided a major impetus for not just reform of the inherent failings of the Safe Harbour agreement itself, but also for surveillance reform. The EU Court assessment of privacy violations focussed in particular on the PRISM surveillance programme conducted by the US National Security Agency (NSA), through which the intelligence agency issues "orders" requesting US companies to turn over data associated with identified users' accounts. This programme is conducted under Foreign Surveillance Intelligence Act (FISA) Section 702, a federal surveillance law that allows the US to engage in surveillance of non-US persons.

In order to ensure that EU residents data in the US is given an adequate level of protection, Section 702 must be substantively reformed prior to ratification of any new data transfer mechanism. Reforms should also extend to other broad surveillance mechanisms that govern surveillance of EU citizens. For example, Executive Order 12333 establishes provisions for the collection, retention, and dissemination of information of users around the world. This Order has provided the basis for, among myriad of other things, the National Security Agency's collection of unencrypted information in transit from Google and Yahoo data centers. Such collection is in direct contradiction to the

[5] FREE Group, EU-US Umbrella Data Protection Agreement : Detailed analysis by Douwe Korff
http://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/
[6] Estelle Massé, Five things you should know about the EU-US Umbrella Agreement
https://www.accessnow.org/five-things-you-should-know-about-the-eu-us-umbrella-agreement/

CJEU ruling, as it inherently poses a threat to the privacy of European Union citizens that use services provided by these and other US companies.

The US Congress has an important role to play here. Unfortunately, the invalidation of Safe Harbour has not yet prompted work to get these reforms adopted. Worse still, legislation that potentially negates the possibility of a future transatlantic data transfer agreement was passed: the Cybersecurity Act of 2015.[7] The passage of the Cybersecurity Act increases the breadth of US spying and further cements the corporate-intelligence relationship.[8] This law would require the Department of Homeland Security (DHS) to deliver "cyber threat" indicators, which are shared with the agencies to intelligence and law enforcement agencies in near real-time. Companies would be granted broad legal immunity for supplying those indicators to the US government, which could include personal information. The option exists to transfer the information entirely secretly. That means massive repositories of personal information, including data transferred from the EU, could be turned over to spying agencies.

Despite these significant problems, the Cybersecurity Act of 2015 passed as Division N of the Consolidated Appropriations Act, also known as the Omnibus act.[9] The Omnibus is a 1.8 trillion dollar tax and spending bill Congress passed to prevent a government shutdown and fund the government through the next fiscal year. By inserting the Cybersecurity Act into "must pass" legislation, Congressional leadership avoided a free vote on the legislation and thereby all but ensured passage. In addition to passing the Cybersecurity Act, the omnibus also included limitations on the authority of the Privacy and Civil Liberties Oversight Board (PCLOB), potentially reducing the effectiveness of the oversight agency. Agencies can now withhold information from the PCLOB, restricting the Board's ability to fulfill its oversight duties.[10]

Oversight powers are especially important if we consider the several occasions on which the US Congress has been misled when reforming or passing legislation. For instance, former NSA Director General Keith Alexander told untruths to members of Congress when testifying on Agency surveillance programmes, and Director of National Intelligence Jim Clapper misled the US Congress when saying that the US government does not "wittingly" collect information about millions of US persons.[11] [12] Intelligence leadership has been no more forthcoming with details of surveillance of non-US persons. Former Speaker of the House John Boehner also made inaccurate statements

---

[7] Drew Mitnick & Estelle Massé, CISA — The biggest threat to the future of transatlantic data sharing
https://medium.com/@dmmitnick/cisa-the-biggest-threat-to-the-future-of-transatlantic-data-sharing-675cc4de670d
[8] Nathan White, Access Now denounces passage of "cyber surveillance" bill in omnibus
https://www.accessnow.org/access-now-denounces-passage-of-cyber-surveillance-bill-in-omnibus/
[9] Nathan White, Access Now denounces inclusion of CISA text in omnibus spending bill
https://www.accessnow.org/access-now-denounces-inclusion-of-cisa-text-in-omnibus-spending-bill/
[10] Coalition Letter on PCLOB access to information
http://www.constitutionproject.org/wp-content/uploads/2015/12/Coalition-Letter-on-PCLOB-Access-to-Information.pdf
[11] EFF, The Top 5 Claims That Defenders of the NSA Have to Stop Making to Remain Credible
https://www.eff.org/deeplinks/2014/06/top-5-claims-defenders-nsa-have-stop-making-remain-credible
[12] The Hill, Attorney: Spy chief had 'forgotten' about NSA program when he misled Congress
http://thehill.com/policy/technology/241508-spy-head-had-absolutely-forgotten-about-nsa-program

about the NSA's surveillance programmes and reportedly, along with other members of congressional leadership, threatened to block strong reform.[13] To date, none of the officials that misled Congress and the public about the very existence of these programmes have been prosecuted or otherwise sanctioned.What is more, laws passed by Congress appear to be abused by agencies. Jim Sensenbrenner, named author of the USA PATRIOT Act, made repeated calls to end these abuses: *"The administration claims authority to sift through details of our private lives because the Patriot Act says that it can. I disagree. I authored the Patriot Act, and this is an abuse of that law."*[14] [15] Similarly, US federal judge John D. Bates publicly accused the National Security Agency of "repeatedly misleading" the FISA Court.[16]

While expanding its surveillance capabilities, the US government has also failed to pass comprehensive data protection legislation at the federal level. Currently, a patchwork of federal and state laws provide inconsistent protection for data that varies by business sector -- such as banking, health, and child safety -- and suffers from significant gaps. In the absence of a federal data breach notification law, various states require companies to notify users of data breach, but no minimum federal standard exists. In sum, inadequate US data protection law leaves users in the dark and more at risk.

Additionally, the United States must respect the human rights of non-US persons by applying internationally accepted human rights standards, such as the International Covenant on Civil and Political Rights (ICCPR), to its surveillance practice. The ICCPR is a United Nations treaty that entered into force in 1976. The Covenant has 74 signatories and 168 state parties. Article 17 states, "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation," and Article 19 states, "everyone shall have the right to hold opinions without interference." Both of these articles should inform US policies on data protection and respect for privacy. However, in 1995 the US State Department took the official position that the Covenant would not be "regarded as having extraterritorial application." This position is contrary to the international majority view of the ICCPR, as well as the official interpretation of the treaty by the Human Rights Committee, that widely takes as given that the treaty applies to state action that impacts people outside of domestic borders.[17] A commitment by the United States to recognise and abide by the international applicability of the fundamental privacy rights enshrined in the ICCPR should inform any reformulated Safe Harbour scheme. Finally, we are concerned that, in breach of international human rights law, the US does

[13] Nathan White, Better than nothing. Less than we deserve.
https://www.accessnow.org/better-than-nothing-less-than-we-deserve/
[14] The Guardian, This abuse of the Patriot Act must end
http://www.theguardian.com/commentisfree/2013/jun/09/abuse-patriot-act-must-end
[15] Note: The USA FREEDOM Act of 2015 ended the programme under §215 of the USA PATRIOT Act that Jim Sensenbrenner was specifically referring to, but other abused programmes remain ongoing.
[16] Charlie Savage and Scott Shane, Secret Court Rebuked N.S.A. On Surveillance
http://www.nytimes.com/2013/08/22/us/2011-ruling-found-an-nsa-program-unconstitutional.html
[17] Douwe Korff, The rule of law on the Internet and in the wider digital world
http://www.coe.int/t/dghl/standardsetting/media/cdmsi/Rule_of_Law_Internet_Digital_World.pdf

not extend certain crucial constitutional guarantees, in particular the Fourth Amendment to its Constitution, to "non-US-persons".[18]

The EU context

At the EU level, the elephant in the room must be addressed: namely Member States' surveillance. While the EU has traditionally been a standard setter in terms of privacy legislation and will shortly conclude its major Data Protection Reform, a large number of EU countries have recently adopted or are in the process of adopting privacy-invasive legislation, enabling government mass surveillance.[19] [20] Governments have the duty to protect human rights, including the right to privacy, and cannot be given *carte blanche* when legislating. This also applies in relation to the – in our view highly contentious – "national security exemptions" in the EU treaties. These exemptions cannot and should not be read as meaning that personal data subject to EU law can be diverted to processing for - often ill-defined - "national security" purposes without regard to the treaties or the EU Charter. On the contrary, the meaning and scope of the exemptions are matters for judicial interpretation; and in any case, as a basic principle of international law, Member States may not rely on these exemptions to act contrary to their general obligations under Union law, including their commitments to human rights and the Rule of Law.

We recently called on EU legislators to learn from past mistakes.[21] Citizens had to wait eight years for the Data Retention Directive to be invalidated, and 15 years for the Safe Harbour to be suspended. While the EU Court and the European Court of Fundamental Rights has proven to be an invaluable backstop, faced with breaches of fundamental rights, repairing mistakes from the EU and national legislature, it is impossible for citizens to get redress for the many years that their human rights have been violated and such abuses can continue with apparent impunity. Unless EU Members States reform their surveillance legislation, EU residents' personal data will not be safe from government spying.

Beyond surveillance, the Schrems case was also about the enforcement and oversight mechanisms of the Safe Harbour. The complainant, Max Schrems, had no other choice but to bring his data protection complaint to the EU Highest Court for remedy. Any future transatlantic data transfer agreement must look closely at this issue by strengthening oversight and providing a meaningful redress mechanism.

The invalidation of the Safe Harbour confirms that the decision to allow the transfer of data outside the EU and their supervision cannot be left to the discretion of the Commission alone. Under

[18] Douwe Korff, The rule of law on the Internet and in the wider digital world
http://www.coe.int/t/dghl/standardsetting/media/cdmsi/Rule_of_Law_Internet_Digital_World.pdf
[19] Lucie Krahulcova, We will, we will, watch you: codifying mass surveillance in France
https://www.accessnow.org/we-will-we-will-watch-you-codifying-mass-surveillance-in-france/
[20] Amie Stepanovich, UK Courts hacking away at surveillance powers
https://www.accessnow.org/uk-courts-hacking-away-at-surveillance-powers1/
[21] Estelle Massé, Access Now testifies on mass surveillance at European Parliament
https://www.accessnow.org/access-now-testifies-on-mass-surveillance-in-the-eu-at-european-parliament/

political pressure, the Commission chose to ignore the concerns raised by the EU Parliament and Data Protection Authorities when adopting the Safe Harbour and chose to defend privacy-limiting legislation adopted by the EU during legal challenges (Safe Harbour and the Data Retention Directive) despite knowing about their shortcomings in both cases – even to the extent of publicly praising itself for this failure in relation to the latter instrument.[22] Therefore, the Parliament must be involved in the negotiations and adoption of any future agreement and EU data protection authorities must be given the necessary means to enforce and oversee the rules.

The conclusion of a robust new transatlantic data transfer agreement that would resist legal challenge in absence of the abovementioned reforms seems impossible. While those reforms must be conducted swiftly, the current time limit for a bilateral agreement on data transfer between the EU and the US by the end of this month is untenable and weakens Europe's negotiating position. In this interim, we encourage Data Protection Authorities to provide companies with further guidance on how to be able to operate by transferring data between the EU and the US without infringing on citizens rights to data protection and privacy. Enforcement action against large companies whose data transfer have currently no legal base, particularly in sectors where the risks are highest - particularly in relation to companies that have no direct relationship with data subjects - should be considered by data protection authorities.

For more information, please contact Estelle Massé at estelle@accessnow.org and Joe McNamee at joe.mcnamee@edri.org

[22] European Commission, Data retention directive: Commissioner Malmström's statement on today's Court judgment http://europa.eu/rapid/press-release_STATEMENT-14-113_en.htm