

Contribution to the European Commission's consultation on a possible EU-US international agreement on personal data protection and information sharing for law enforcement purposes

Summary

1. The transfer of personal information to the United States currently entails the real risk of a violation of the human rights guaranteed in the ECHR and is therefore illegal. An international agreement cannot not remove that risk.
2. For as long as the sharing of information with the United States is still taking place (e.g. judicial cooperation, PNR data), an international agreement with the US would be an improvement over the current situation if it does not in itself authorise information sharing but applies exclusively to the information sharing that is taking place under existing agreements, thus reducing the amount of information shared and providing for more safeguards.
3. Information about people may be handed over to states that protect fundamental rights, as regards both the substantive guarantees offered and the mechanisms controlling their observance, in a manner which can be considered at least equivalent to that for which the ECHR provides, unless in a particular case there is a real risk that the transfer may ensue a violation of human rights.
4. Information relating to a person may be handed over to states that do not protect fundamental rights in an equivalent manner only if in every single case it is ascertained that the transfer does not violate the ECHR and does not ensue a violation of human rights at a later stage (e.g. torture and cruel, inhuman or degrading treatment; targeted killings or death penalty; deprivation of a fair trial; extrajudicial arrest and detention).

To comply with the right to privacy, certain guarantees must be laid down in self-executing provisions of the law of both the sender and recipient states, applying both to the information that is to be passed on and to any personal information that was obtained as a result of the data transfer:

- a) Strict conditions: Information relating to people should be disclosed to foreign agents and states only for the purpose of prosecuting a criminal act (according to the law of both countries) the person concerned is suspected of on the basis of specific facts, and which is likely to lead to a prison sentence of four years or more for the person concerned. Only information that is adequate, necessary and proportionate for prosecuting that criminal act may be transferred.
- b) Sensitive information: Special protection must be afforded to sensitive information.

- c) Compliance: In order to ensure compliance with these safeguards, the decision on any transfer of information as well as on its use should be taken by an independent and impartial tribunal.
 - d) Restrictive and specific purpose limitation: After the transfer, personal information must not be used, passed on or retained for any purpose (investigation etc.) other than that which it was obtained for.
 - e) Deletion: Personal information must be destroyed when not or no longer necessary for the specific purpose (investigation) it was obtained for. It must also be destroyed if it was obtained or is being held illegally.
 - f) Independent oversight: A public authority, acting with complete independence, must ensure the legality of any processing of personal information.
 - g) Notification: An individual whose data is processed without their knowledge must be notified as soon as the purpose of the processing will allow.
 - h) Data subject rights: Everyone must have a right to find out which information is being held relating to them, as well as a right to have incorrect information corrected and illegally obtained or held information deleted.
 - i) Effective remedy: Everyone whose rights as set forth above are violated must have the right to an effective remedy before an independent and impartial tribunal notwithstanding that “state secrets” would need to be disclosed or that the violation is considered a matter of “national security”.
5. Non-public legal entities must not transfer personal information to states that reserve access to the information without having in place the safeguards and respecting the conditions set out above.

A. Foreword

The European Convention on Human Rights (ECHR) constitutes a “constitutional instrument of European public order” in the field of human rights.¹ As elements of that public order, the rights guaranteed in the Convention are not subject to derogation and prevail over any other interest (*ius cogens*).

The handing over of personal information to states that are not a party to the ECHR constitutes a most grave interference with the rights of the individuals concerned. As a result of the data transfer, the individual loses control over the use that is made of their information. The recipient state is not bound by the European instruments for the protection of human rights. The transfer may thus, *inter alia*, lead to the secret gathering of more information and secret surveillance, to the inclusion in

¹ ECtHR, *Bosphorus v. Ireland*, judgement of 30 June 2005, § 156.

no-fly or watchlists, to the freezing of assets, to limitations of travel, to arrest and interrogation, to abduction and rendition to third states, to torture, degrading treatment or even to execution (death penalty, targeted killings), both by agents of the recipient state and of states it passes information on to (e.g. US-Philippines).

On the other hand, the Commission's contention that “[t]he transfer of personal data is an essential element of transatlantic law enforcement cooperation in order to fight serious transnational crime and terrorism effectively” is incorrect. Particularly in view of the existing agreements on mutual assistance in criminal matters, the present legal framework warrants an appropriate level of protection from crime in Europe. Although sharing more information may be considered useful in particular cases by some authorities, there is no evidence that it would decrease crime rates and thus enhance our safety in a statistically significant measure. In view of that, the importance of human rights as a means to ensure the safety and integrity of the person outweighs any interest authorities may have in an ever expanding gathering and use of personal information for “law enforcement purposes”.

B. The transfer of personal information to states with equivalent protection of fundamental rights

It is in line with the ECHR to transfer information about people to states that protect fundamental rights, as regards both the substantive guarantees offered and the mechanisms controlling their observance, in a manner which can be considered at least equivalent to that for which the ECHR provides,² unless in a particular case there is a real risk that the transfer may ensue a violation of human rights.³ The United States, for the reasons set out in detail below, do not protect fundamental rights in an equivalent manner.

C. The transfer of personal information to other states, especially to the US

Information relating to a person may be handed over to states that do not protect fundamental rights in an equivalent manner only if in every single case it is ascertained that the transfer does not violate the ECHR and does not ensue a violation of human rights at a later stage. Information must not be passed on where the transfer would entail the real risk of a violation of a human right as guaranteed in the ECHR (e.g. prohibition of torture and cruel, inhuman or degrading treatment, right to life and prohibition of death penalty; right to fair trial; protection from unlawful detention).

It is self-evident that the passing on of personal information to foreign agents must be in line with the ECHR. It is less evident that in examining that issue, the way the information is used abroad must be taken into account.

² ECtHR, *Bosphorus v. Ireland*, judgement of 30 June 2005, § 155.

³ ECtHR, *Bosphorus v. Ireland*, judgement of 30 June 2005, § 156.

The European Court of Human Rights has held Contracting States responsible for acts which have sufficiently proximate repercussions on rights guaranteed by the Convention, even if those repercussions occur outside their jurisdiction.⁴ For example, a Contracting State must not knowingly hand over a fugitive to another State where there are substantial grounds for believing that the fugitive faces a real risk of being subjected to torture or to inhuman or degrading treatment or punishment.⁵ The same applies for other human rights that risk to be violated abroad, including – but not limited to – the right to privacy.

The Supreme Court of Canada ruled in 2009 that Canada was banned from “participating in a process that was violative of Canada’s binding obligations under international law” and that a process conducted by the US at Guantanamo Bay “violated Canada’s binding obligations under international law”. Although the Court did not, in the case at hand, find it “necessary to conclude that handing over the fruits of the interviews in this case to U.S. officials constituted a breach of Mr. Khadr’s s. 7 rights” to life, liberty and security, there can be no doubt that the information sharing was considered illegal by the Court. It can make no difference whether information sharing contributes to ongoing human rights violations or whether it prompts such violations in a way that was foreseeable for the authorities sharing the information.

The Eminent Jurists Panel's 2009 report on Terrorism, Counter-terrorism and Human Rights confirms that “[i]f [...] State agencies are systematically sharing information with countries and agencies with a known record of human rights violations, it is difficult to resist the argument that States are complicit, wittingly or unwittingly, in the serious human rights violations committed by their partners in counter-terrorism.”⁶

Applying these principles to the US, no personal information may currently be transferred to the United States as any data transfer entails the real risk of a violation of a human right as guaranteed in the ECHR. Firstly, the processing of information in the US violates the human rights to the protection of personal data and to effective remedy. Secondly, the United States routinely violate human rights in operations outside its territory. Both is explained in more detail below.

1. US compliance with human rights

In its resolution regarding the EU-USA judicial cooperation agreement the European Parliament confirmed that “full respect for the ECHR” is essential to any agreement on cooperating with foreign states, meaning that the minimum guarantees afforded by the ECHR must exist in the recipient state as well. The European Parliament however found that „the judicial system of some US States does not offer the same level of guarantees that the ECHR and EU measures seek to provide for EU Member States“,⁷ meaning that personal information cannot at present lawfully be provided to the US.

4 ECtHR, *Ilascu v. Moldova*, judgement of 8 July 2004, § 317.

5 ECtHR, *Ilascu v. Moldova*, judgement of 8 July 2004, § 317.

6 <http://ejp.icj.org/IMG/EJP-Report.pdf>, 85.

7 European Parliament recommendation to the Council on the EU-USA agreements on judicial cooperation in criminal matters and extradition (2003/2003(INI)), A5-0172/2003.

United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, identified in 2007 “serious situations of incompatibility between international human rights obligations and the counter-terrorism law and practice of the United States. Such situations include the prohibition against torture, or cruel, inhuman or degrading treatment; the right to life; and the right to a fair trial. He has also identified deficiencies in United States law and practice pertaining to the principle of non-refoulement; the rendition of persons to places of secret detention; the definition of terrorism; non-discrimination; checks in the application of immigration laws; and the obtaining of private records of persons and the unlawful surveillance of persons, including a lack of sufficient balances in that context.”⁸

In its comments on the report⁹ the United States reiterated its view according to which

- human rights did not apply to dealings of US agents outside the territory of the United States of America,
- “unlawful enemy combatants” neither enjoyed the rights of civilians nor those of prisoners of war under the Geneva Convention,
- individuals who never breached any law might be arrested and deprived of their liberty in the course of a “war on terror” without being entitled to a fair and public hearing within a reasonable time before a regular tribunal, and to a lawyer,
- the “war on terror” was covered by the law of armed conflict while human rights such as those guaranteed in the International Covenant on Civil and Political Rights did not apply,
- operations in the course of the “war on terror” were not subject to judicial review,
- the aforesaid applied in the same way to children,
- extraterritorial detention centres such as the one at Guantanamo Bay would continue to be operated until an alternative has been found,
- “military commissions” were entitled to sentence “unlawful enemy combatants” to death,
- the notion of torture was limited to what is prohibited under the US constitution [the methods of interrogation thus applied by US agents include exposure to stress positions, extreme temperature changes, sleep deprivation, and “waterboarding”],
- the extrajudicial, targeted killing of “enemy combatants” was permitted in the “war on terror”,
- the rendition of individuals to foreign states was not limited to subjecting them to a fair trial,

8 Report of 22 November 2007, A/HRC/6/17/Add.3, <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G07/149/55/PDF/G0714955.pdf?OpenElement>.

9 <http://weblog.leidenuniv.nl/media/blogs/76039/1948/Scheinin-Response-HRC%5B1%5D.pdf>.

- the surveillance of telecommunications by suspected members “of al Qaida or an affiliated terrorist organization” was permitted without a legal basis and without judicial authorization.

Under Barack Obama's presidency, the US still

- maintains the “war on terror” paradigm as a justification for imprisoning individuals indefinitely without charge,
- authorises “military commissions” to impose sanctions on individuals without satisfying minimum judicial standards to warrant a fair trial,
- abducts individuals and renders them to countries where they face a serious risk of torture, relying blindly on non-binding “diplomatic assurances”,
- broadly uses the “state secrets” privilege to have litigation before US courts for human rights violations dismissed.¹⁰

In view of the systematic violation of fundamental human rights by the United States, any transfer of personal information to the US risks entailing more such violations. Therefore, transfers of personal information to the United States are not permitted under the ECHR and the EU Fundamental Rights Charter at present.

Agreements with or even mere diplomatic assurances on the part of the United States cannot remove the real risk of ensuing human rights violations. First of all, the US executive is legally unable to provide all necessary guarantees, such as independent oversight and effective judicial remedy. Secondly, agreements with the executive branch of government cannot effectively be enforced by the individual concerned. Human rights instruments require effective mechanisms for ensuring their observance.

2. The human right to privacy

In order to ensure compliance with the human right to privacy when sharing personal information, inter alia the following guarantees must be in place:

a. Conditions for the transfer of personal information

According to the principle of proportionality, the transfer of information and its consequences may not be excessive in relation to its benefits to society. The principle of proportionality is guaranteed both under the ECHR and the Charter of Fundamental Rights (Art. 52).

The handing over of personal information to states that are not bound by the ECHR constitutes a grave interference with the right to privacy as has been explained above. In view of that, personal information may be handed on to states that are not party to the ECHR only in exceptional cases and subject to strict guarantees:

¹⁰ Human Rights Watch: Counterterrorism and Human Rights. A Report Card on President Obama's First Year (14 January 2009), <http://www.hrw.org/en/news/2010/01/14/counterterrorism-and-human-rights-report-card-president-obama-s-first-year>.

- i. Information relating to people should only be transferred on a case by case basis for the purpose of prosecuting a serious criminal act (according to the law of both countries) the person the information relates to is suspected of on the basis of specific facts. A criminal act should be considered serious only if it is likely to attract a prison sentence of four years or more.
- ii. Only information that is adequate, necessary and proportionate for prosecuting that criminal act may be transferred. According to the ECHR, personal data must be relevant and not excessive in relation to the purposes for which it is processed.¹¹
- iii. Special protection must be afforded to sensitive information. Sensitive information is information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, concerning health or sex life, information resulting from interferences with the inviolability of the home, with the secrecy of telecommunications, concerning professional secrets and resulting from interferences with personal relationships of trust (family members).
- iv. Information relating to the core sphere of privacy must not be disclosed at all.
- v. In order to ensure compliance with these safeguards, the decision on any transfer of information as well as its use should be taken by independent and impartial tribunals. According to the ECHR, interference by the executive authorities with an individual's rights that the individual has no knowledge of must be subject to effective supervision, which should normally be carried out by the judiciary.¹²

The conditions set out above are necessary to meet the principle of proportionality where transferring personal information to states that are not bound by the ECHR.

Where information is received from such states, the recipient state must examine whether those conditions are met. Information which could not have legally been obtained or stored in Europe must not be requested, stored or used by European authorities in any way.

b. Conditions for the processing of transferred personal information

As set out above, no transfer of personal information must take place that would risk ensuing a violation of human rights, including the right to privacy. Therefore, personal information may be handed on only to states that provide guarantees relating to the further processing of information that was shared. The following conditions not only apply to the information that was passed on originally but also to any personal information that was gathered or processed as a result of that data transfer.

- i) **Purpose limitation:** Recipient states must not use, transfer or retain personal information for any purpose (investigation procedure) other than that which it was obtained for (restrictive and specific purpose limitation).

¹¹ ECtHR, *S. and Marper v. UK*, judgement of 4 December 2008, § 103.

¹² ECtHR, *Rotaru v. Romania*, judgement of 4 May 2000, § 59.

Principle 1 as set out in the Annex to the HLCG report of May 2008 (“Purpose Specification/Purpose Limitation”) does not provide for restrictive and specific purpose limitation in that sense and thus fails to satisfy human rights requirements to the disclosure of personal information to foreign agents and states.

- ii) **Deletion:** The information must be destroyed when not or no longer necessary for the specific purpose (investigation) it was obtained for or if it was obtained or is being held illegally. According to the ECHR, personal information must be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.¹³

The Principles developed by the HLCG do not provide for an enforceable right to deletion and thus fail to satisfy human rights requirements.

- iii) **Oversight:** A public authority, acting with complete independence, must ensure the legality of any processing of personal information. This is provided for in Art. 8 of the Fundamental Rights Charter.

The current US system of oversight does not provide for complete independence and thus does not comply with human rights exigencies. Principle 7 as set out in the Annex to the HLCG report of May 2008 (“Independent and Effective Oversight”) does not provide for complete independence and thus fails to satisfy human rights requirements.

- iv) **Notice:** An individual whose data is collected or passed on without their knowledge must be notified as soon as the purpose of the processing will allow. According to the ECHR, as soon as notification can be made without jeopardising the purpose of the measure, information should be provided to the persons concerned.¹⁴

US law does not at present reliably provide for an enforceable right to individual notification as required by the ECHR. Nor does Principle 9 as set out in the Annex to the HLCG report of May 2008 (“Transparency and Notice”) as the right to notification is made subject to a “requirement by law”, does not guarantee an individual notice and is to apply only “insofar as is necessary to ensure fairness”. This principle thus fails to satisfy human rights requirements.

- v) **Data subject rights:** Everyone must have a right to find out which information is being held on them, as well as to have incorrect information corrected and illegally held information deleted. According to Art. 8 of the Charter of Fundamental Rights of the European Union, everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

Principle 8 as set out in the Annex to the HLCG report of May 2008 (“Individual Access and Rectification”) does not include a right to have illegally held information deleted as it only provides for “rectification and/or expungement” of personal information. This principle thus fails to satisfy human rights requirements.

¹³ ECtHR, *S. and Marper v. UK*, judgement of 4 December 2008, § 103.

¹⁴ ECtHR, *Association for European Integration v. Bulgaria*, judgement of 28 June 2007, § 90.

3. The human right to effective remedy

Everyone whose rights as set forth above (e.g. preconditions, purpose limitation, access right, right to deletion, right to independent supervision) are violated must have the right to an effective remedy before an independent and impartial tribunal notwithstanding that what the state claims “secrets” would need to be disclosed or that the violation is claimed to be a matter of “national security”.

The right to an effective remedy before a tribunal is guaranteed in Art. 13 ECHR and in Art. 47 of the Charter of Fundamental Rights of the European Union. As explained above, Europe is responsible for the foreseeable consequences of passing on information to foreign agents. European Courts cannot provide for effective remedy for violations that occur after personal information has been passed on. Therefore, the transfer of personal data can satisfy human rights only if the recipient states' legal system provides for effective remedy.

The judicial system of the United States does not at present provide effective remedy:

- a. International agreements are not self-executing in the United States at present and can therefore not be applied by or invoked before US courts.
- b. It is unclear whether US courts will review acts by government officials performed outside the territory of the United States.
- c. The “state secrets doctrine” allows the US government to have any action struck down with the claim that court proceedings might disclose sensitive information which might in turn endanger national security.¹⁵ So far all actions for human rights violations in the “war on terror” have been squashed in that way, depriving the individuals concerned of any remedy.

The redress principle as set out in the Annex to the HLCG report of 28 October 2009 does not satisfy human rights either as it merely provides for administrative redress and does not address the constitutional deficiencies in the US set out above.

D. Transfer by non-public legal entities

With relation to directive 95/46/EC, it should be mentioned that non-public legal entities may not transfer personal information to states that reserve access to the information by public authorities without observing the principles set out above. When examining whether an equivalent level of data protection is ensured within the meaning of directive 95/46/EC, it is often overlooked that information transferred abroad is exposed to the risk of access by public authorities. Where public access to privately held data risks ensuing violations of human rights, no transfer of data may take place.

As explained above, transfers of data to the United States of America risk ensuing violations of human rights. The US excessively collect and retain privately held information on non-US citizens (“national security letters”, “data warehouses”), thereby violating the human right to privacy as well as other human rights.

¹⁵ http://en.wikipedia.org/wiki/State_Secrets_Privilege.

E. Conclusions

Both the legal framework and the practices of the United States of America are fundamentally at odds with human rights as recognised in the ECHR, the EU Fundamental Rights Charter and the International Covenant on Civil and Political Rights. The changes that are needed to ensure that information sharing with the US will not result in human rights violations affect US national security policy and go beyond what even a comprehensive agreement with the US could achieve.

The EU must therefore strongly reject any sharing of personal information with the United States at present and in the foreseeable future. Instead the EU should recommend the US ratify in a self-executing manner the International Covenant on Civil and Political Rights including its First Optional Protocol as well as the American Convention on Human Rights. Once these instruments have been implemented, the legality of information sharing with the United States could be reassessed.

Without prejudice to this position, for as long as the sharing of information with the US is taking place (e.g. judicial cooperation, PNR data) despite the shortcomings set out above, an international agreement with the US on personal data protection would be an improvement over the current situation if the agreement does not in itself authorise information sharing but applies exclusively to information that is being shared under existing agreements, thus reducing the amount of information shared and providing for more safeguards. An international agreement with the US authorising information sharing beyond current treaties must not be negotiated or ratified.

06/03/10