Privacy International response to consultation on the interoperability of EU information systems for borders and security

Via email: HOME-INTEROPERABILITY@ec.europa.eu

Privacy International welcomes the opportunity to respond to this consultation. Established in 1990, Privacy International is a non-profit, non-governmental organisation based in London, dedicated to defending the right to privacy around the world.

To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional and international laws that protect privacy around the world. It has litigated or intervened in cases implicating the right to privacy in the courts of the United States, the UK, and Europe, including the European Court of Human Rights and the European Court of Justice. It also strengthens the capacity of partner organisations in developing countries to identify and defend against threats to privacy. Privacy International employs technologists, investigators, policy and advocacy experts, and lawyers, who work together to understand the technical underpinnings of emerging technology and to consider how existing legal definitions and frameworks map onto such technology.

Introduction

The stated aim of the 'consultation on the interoperability of EU information systems for borders and security' is to explore how the information systems in the European Union can enhance border management and internal security. An additional aim is efficiency and cost savings.

A feature of this is to seek interoperability between the EU information system in the areas of borders and security: Schengen Information System (SIS); Visa Information System (VIS); Eurodac; Entry-Exit System (EES); European Travel Information and Authorisation System (ETIAS) and European Criminal Records Information System – Third Country Nationals (ECRIS-TCN). There is a lack of detail or consideration whether this will actually achieve the stated aim in respect of borders and security and cutting costs. Without access to a finalised impact assessment which includes technical reviews we do not believe that this case has been made.

It is concerning that the consultation document, in noting the 'structural shortcomings in the EU's current information landscape[1]' makes no statement at the outset in relation to privacy, data protection and cyber security regarding the

[1] Sub-optimal functionalities in some of the existing information systems;
Information gaps in the EU's architecture of data management;
A complex landscape of differently governed information systems; and
A fragmented architecture of data management for borders and security where information is stored separately in unconnected systems, leading to blind spots.

current information landscape. In the stated objectives[2] the consultation fails to explicitly mention protecting against the harms and risks associated with interoperability and the retention of data in these systems which will be accompanied by broad access throughout the European Union.

We respond in order to raise summary concerns in relation to significant potential harms associated with collection, retention, and use of personal data; vast access rights; and the creation of more integrated databases. The plans either for a single database or so-called 'targeted approach' both pose a risk to individual privacy and data security. We submit that before embarking on costly, ambitious and complex program of interoperability, a strong case must be made for necessity and proportionality of the proposal and full details must be published. Further such an ambitious and risky proposal should be subject to rigorous independent review.

We have not answered the questions and are concerned that responses are sought to questions which are accompanied by a paucity of detail as to how proposals will work in practice and in the absence of an appropriate impact assessment. In these circumstances it is not possible to provide informed responses to those questions.

Summary concerns

1. Unnecessarily intrusive, risk of profiling and discrimination

The European databases involve the gathering and storing of a wide variety of types of information, including sensitive biometric information such as fingerprints, facial images and biometric data from Europol and/or Interpol. The 'targeted approach' proposes a shared biometric matching service. The Common Identity Repository would 'complement the shared biometric matching service bringing together alphanumeric data, such as names and dates of birth, that have been stored in the various information systems for border management and security.

The broad scope of data requested from those whose data will be included within interoperable databases, seems unnecessarily intrusive, interfering with fundamental human rights. The objectives fail to elaborate on the impact on data protection rights and the right to privacy. These rights and related issues should be front and centre of any plan in respect of information systems and databases.

Extensive access exists and is planned for the information systems. The end-users include border guards, law enforcement officers, immigration officials, customs officers, visa officials and judicial authorities. Users can search biometric data "from all sources".

---

[2] Enhancing interoperability between information systems is considered to be fundamental to address the above challenges. Specific objectives would be the following:

- Ensuring that end-users, particularly border guards, law enforcement officers, immigration officials and judicial authorities have fast and seamless access to information in various systems.
- Facilitating and streamlining access by law enforcement authorities to non-law enforcement information systems for prevention, investigation, detection or prosecution of criminal offences.
- Facilitating a solution to detect and combat identity fraud

The range of data collected and the wide scope for its use give rise to concerns that data may be used for profiling with potentially discriminatory consequences, as recognised by the EU Fundamental Rights Agency.[3]

We are concerned that systems proposed which entail a central registry of sensitive personal data such as biometric data raise substantial issues in the context of the history of identification systems throughout the world, which provides evidence of 'function creep'.

It has been noted in relation to ETIAS alone, that it should be conceived of as a platform for mining and profiling personal data, rather than just a platform for issuing automated or manual travel authorisation decisions. The ETIAS screening rules aim to identify persons who are otherwise unknown to responsible authorities of the Member States but are assumed to be of interest for irregular migration, security or public health purposes. These persons are flagged not because of specific actions they have engaged in but because they display category traits[4].

The implications of interoperability to the fundamental rights of individuals will be magnified when compared to the current compartmentalisation of databases; the specific purposes for which the systems were set up will be nullified; and there is a risk of extensive profiling, as authorities may be able to compile a profile of travellers on the basis of information from systems.

2. Lack of consideration and emphasis on data retention safeguards

Key safeguards around retention and access of data must be considered to avoid risks associated with indiscriminate collection and access that risks abuse of power. Absence of limitations on retention (e.g. the absence of proper deletion mechanisms for irrelevant information or of proportionate retention periods) increases the likelihood for security breaches and for unauthorised access.

Similarly, broad, vague or ill-defined rules on access to retained data can lead to unlawful surveillance, a rise in collateral data (the incidental access to information of individuals who are not related to the subject of the investigation), misuse and other abuses of data protection standards (e.g. sharing of personal data).

Consequently, safeguards must be put in place to ensure that the interference with fundamental rights is minimised at both the retention and access stages.

The human rights standards on data retention developed by the CJEU, the European Court of Human Rights (to which all EU Member States are also bound, by their being parties to the European Convention on Human Rights) and the UN

[3] http://fra.europa.eu/en/publication/2017/fundamental-rights-interoperability

[4] http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583148/IPOL_STU(2017)583148_EN.pdf

human rights mechanisms, seek to ensure that the individuals whose data is being retained are adequately empowered to protect themselves against associated risks.

In two judgments, the *Digital Rights Ireland* case (2014) and the more recent *Tele-2/Watson* decision (2016), the Court of Justice of the European Union (CJEU) reaffirmed the requirement that all data retention regimes must comply with the principles of legality, necessity and proportionality.

In Digital Rights Ireland, the CJEU held Directive 2006/24 to be invalid as a disproportionate exercise of the EU legislature's powers in breach of Articles 7, 8 and 52(1) of the EU Charter of Fundamental Rights.[5] In that case the CJEU recognised that

> "the persons whose data have been retained [must] have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data."[6]

All EU Member States are parties to the European Convention on Human Rights and Fundamental Freedoms and to the International Covenant on Civil and Political Rights (ICCPR), both enshrining the right to privacy. In its ruling in *Roman Zakharov v. Russia*, the Court emphasised the need for safeguards, in particular clear and proportionate rules about storage and destruction of data:

> "*The Court considers the six-month storage time-limit set out in Russian law for such data reasonable. At the same time, it deplores the lack of a requirement to destroy immediately any data that are not relevant to the purpose for which there has been obtained. The automatic storage for six months of clearly irrelevant data cannot be considered justified under Article 8.*
>
> *Furthermore, as regards the cases where the person has been charged with a criminal offence, the Court notes with concern that Russian law allows unlimited discretion to the trial judge to store or to destroy the data used in evidence after the end of the trial. Russian law does not give citizens any indication as to the circumstances in which the intercept material may be stored after the end of the trial. The Court therefore considers that the domestic law is not sufficiently clear on this point..."*[7]

---

[5] Article 51(2) titled "Scope of Guaranteed Rights" enshrines that "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

[6] Digital Rights Ireland Case, supra note 1, at para. 54.

[7] Roman Zakharov v. Russia, App. No. 47143/06, European Court of Human Rights, Judgment, paras. 255-256 (4 December 2015).

3. Overly ambitious, complex and risk of failure

The proposal cites a varied number of aims to be achieved as a result of interoperability:

- To offer a large and varied type of end-user 'fast and seamless access to information in various systems';
- To provide access by law enforcement to non-law enforcement information systems for prevention, investigation, detection or prosecution of criminal offences;
- Detection and combating identity fraud;
- Avoid duplication of data and reduce overlaps and highlight discrepancies in the data;

Many complex systems do not live up to expectations and with respect to sensitive biometric data held and the demands on the system, this is because they prove unable to cope with the enormous variations among large populations. systems embody greater levels of risk of failure, and resultant vulnerability of organisations and individuals' dependent on them.

Biometric identification relies on technology that is far from proven, and major organisational adjustments are needed to cope with it. There are many practical problems involved in complex and largely automated schemes, and in coping with exceptions, system outages and claims of database error.

4. Lack of clarity and explanation

The inception impact assessment states that a further assessment is to come. The justification for and necessity of the interference have not been clearly explained and therefore this consultation is premature.

It is impossible to assess the proportionality of the proposed measures as the need to be met has not been clearly expressed. There is no indication that alternative less intrusive options have been considered, and the effectiveness of the proposal has not been demonstrated.

We note the recommendations made in relation to the study for the LIBE committee, regarding ETIAS and those of EDPS Opinion on the Proposal For a European Travel Information and Authorisation System (Opinion 3/2017)[8] and encourage reflection on this study in the context of the current proposal[9], as well as the EU Fundamental Rights Agency study on Fundamental rights and the interoperability of EU information systems.[10]

---

[8] https://edps.europa.eu/sites/edp/files/publication/17-03-070_etias_opinion_en.pdf

[9] http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583148/IPOL_STU(2017)583148_EN.pdf

[10] http://fra.europa.eu/en/publication/2017/fundamental-rights-interoperability

5. Failure to consider in detail cyber security issues

Technological systems must support and enhance privacy, not undermine it. If the European Union seeks to implement interoperability in its databases, they must not undermine the security of individuals' data. If the information is not properly protected there is the potential of unauthorised access to troves of information by third parties, including criminals and agents of authoritarian regimes from which individuals have sought asylum in the EU.

There are serious risks when governments build systems that generate and accumulate vast data stores without proper regard to risk, security or data minimisation. The personal information of over 93 million voters in Mexico[11], including home addresses, were openly published on the internet after being taken from a poorly secured government database. This can be highly sensitive information; in Mexico for instance there are gross abuses of rights, including up to 100,000 people are reportedly kidnapped each year[12]. Similarly, the personal information of over 55 million Filipino voters were made publicly available, the biggest data breaches in the Philippines' history[13]. A database containing the records of 650,000 patients in Sao Paolo, Brazil was made public, putting people at a variety of risks, from becoming victims of identity theft to persecution e.g. when the identities of women undergoing abortions were exposed[14].

Privacy International believes that privacy and security are both essential to protecting individuals, including their autonomy and dignity. These systems and their future use risk undermining the privacy and security of individuals, groups and whole communities. Undermining privacy undermines the security of individuals and broader infrastructure.

Too often governments and companies have chosen to undermine privacy through alterations or intentional designs into common and widely-used infrastructure. The existing databases used by the European Union were not designed and implemented at a time when security was a primary consideration.

We are concerned therefore about the security if the proposed systems. We recommend that a detailed technical impact assessment regarding cyber security considerations be finalised and made publicly available before any proposals are implemented.

---

[11] Dell Cameron, Private Records Of 93.4 Million Mexican Voters Exposed In Data Breach, The Daily Dot, 22 April 2016 http://www.dailydot.com/layer8/amazon-mexican-voting-records/

[12] Vladimir Hernandez, Our World: Kidnapped in Mexico, 15 March 2017 http://www.huf ngtonpost.com/vladimir- hernandez/our-world-kidnapped-in-mexico_b_9462258.html

[13] State of Privacy report for The Philippines https://www.privacyinternational.org/node/969#toc-5

[14] State of Privacy report for Brazil https://www.privacyinternational.org/node/979#toc-5

Cyber security should be considered a public good. In a cyber security context, securing the individual helps secure everyone. In order to secure the individual, the priorities should be protecting individuals and their data.

Personal data is valuable. The value of the data is exactly why governments want to collect, access and mine it, and criminals want to steal it, while foreign governments may see intelligence value as well. Gaining access to European information systems could be lucrative in many ways to many parties.

Good cyber security should put people and their rights at the centre, and minimise the risk to individuals and their data. That means limits the collection and processing of data, and the entities who have access. This proposal runs counter to those objectives in too many ways.

6. Artificial Intelligence

The report fails to consider the use of Artificial Intelligence on information collected, retained and processed by the European Union. Artificial Intelligence ("AI") is a term that is often used to refer to a diverse range of applications and use-cases at different levels of complexity and abstraction. The term is employed to encompass everything from machine learning which makes inferences, predictions and decisions about individuals, and other domain-specific AI algorithms to fully autonomous and connected objects.

We are concerned about current and future applications of AI that are designed for the following purposes: (1) to identify and track individuals; (2) to predict or evaluate individuals or groups and their behaviour; (3) to automatically make or feed into consequential decisions about people or their environment; and (4) to generate, collect and share data.

Using machine learning methods, highly sensitive information can also be inferred, or predicted from non-sensitive forms of data.

AI systems can be used to make or inform consequential decisions about people or their environment.

Novel applications and recent advances in artificial intelligence could negatively affect the right to privacy. This is significant since privacy is the lynchpin of indispensable individual values such as human dignity, personal autonomy, freedom of expression, freedom of association and freedom of choice, as well as broader societal norms.

Poor quality data or systematically biased data are common concerns in profiling using machine learning. Yet even if profiling on perfect data, individuals could still be misclassified, misidentified or misjudged and such errors may disproportionality affect certain groups of people.[15]

[15] http://fra.europa.eu/en/publication/2017/fundamental-rights-interoperability

AI-driven applications sort, categorise, assess and rank people often without their knowledge or consent. The United Nations Human Rights Council, on 22 March 2017 noted with concern “that automatic processing of personal data for individual profiling may lead to discrimination or decisions that otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights”.

The data that feeds into AI systems; the data that AI systems generate; as well as how and whether AI systems should be used to make or inform consequential decisions about individuals and groups, must be regulated.

Conclusion

We believe this consultation is premature and there needs to be additional information on the scope and impact of these proposals, particularly with regards to their implication for the right to privacy and to data protection, as well as the related cyber-security risks.