Negative Brief: Database Interoperability – not a problem

By “Coach Vance” Trefethen

***Resolved: The European Union should substantially reform its immigration policy.***

In Status Quo, the EU has recently set up a computer software system that allows a single query by a border guard or law enforcement officer to check multiple separate databases ("interoperability") to search for information about a traveler crossing the border or a suspect in custody. This allows for more accurate identification of security threats and more accurate removal of illegal immigrants. For example, one database might have information that this individual got caught immigrating illegally a few years ago, or was part of a known terrorist organization, while the other databases don't have that info. The officer might not have known to search the specific database that had the important information, but now with "interoperability," with a single search, he finds it quickly. AFF plan cancels this new system and reverts back to the system of separate databases without interoperability.

Negative: Database Interoperability – not a problem 3

BACKGROUND 3

Plan repeals EU regulation 2017/0351 and 0352. 0351 is also known as 32019R0817 because it was updated and amended several times between 2017 and 2019 as shown here: 3

GOAL / CRITERION RESPONSES –"Protecting Privacy" is a useless goal, not valid for deciding the round 3

1. No justification in 1AC 3

They just make assumptions and hope you won't notice 3

2. Privacy is dead and no one cares 4

Nobody cares any more about privacy. You already gave it away when you went on Facebook or got a smart phone 4

Data privacy is pretty much dead 4

3. Reverse voting issue 4

4. Counter-Goal 4

EXTRA-TOPICALITY 5

1. Regulations in the Plan go beyond immigration policy 5

What is Extra-Topicality 5

The Problem: Their Justification 2 on EU citizens gives away the fact that part of their plan is extra-topical 5

Impact: Drop Justification 2 or else award a Neg ballot 5

HARMS / SIGNIFICANCE 5

1. Rights protected outweigh insignificant potential privacy losses 5

Interop rules have safeguards against privacy loss, and they promote better respect for other human rights 5

2. Privacy violations are compensated under current law 6

Any violations of personal data trigger a right to compensation for the victim under the 2019 version of the law AFF wants to repeal 6

3. Only shows data the investigator was allowed to see 6

Don't be confused: The new regulations don't allow the investigator to suddenly see all kinds of secret stuff. He can still only see what he was allowed access to under previous rules 6

4. No one is harmed 6

No one harmed in the 1AC 6

Europeans don't feel harmed: 92% of Europeans agree with Negative. Law enforcement should share more data to fight crime & terrorism 6

SOLVENCY 7

1. Reverting to old database system won't solve security problems 7

The old database system had security holes and data leakages too. Examples from Bulgaria in 2013 and Netherlands in 2011 happened long before the new system was implemented 7

DISADVANTAGES 8

1. Terrorism 8

Link: Without interop, there are delays and inefficiencies when investigating terrorism because authorities don't know in advance which database to look in 8

Link: Interop streamlines access to data to speed up prevention, detection or investigation of terrorism 8

Link: US Dept of Homeland Security agrees with Negative. Sharing information and enhancing access to it was recommended in their National Strategy to Combat Terrorist Travel in 2018 9

Impact: Lost lives. Shorter response time is key to saving lives in a crisis 9

2. Lost human rights and benefits 10

Interop upholds a number of rights better than without it. And it helps solve human trafficking of children 10

3. Increased illegal immigration 10

Link: EU Interop reduces illegal immigration 10

Impact: Lost jobs from illegal immigration 11

Impact: Black market work causes economic and social harm 11

Link: Illegal immigrants destroy native jobs in irregular sectors 11

Negative: Database Interoperability – not a problem

BACKGROUND

Plan repeals EU regulation 2017/0351 and 0352. 0351 is also known as 32019R0817 because it was updated and amended several times between 2017 and 2019 as shown here:

EUR LEX 2019. (official register of European Union laws online) " 2017/0351/COD" published 22 May 2019 https://eur-lex.europa.eu/procedure/EN/2017\_351



GOAL / CRITERION RESPONSES –"Protecting Privacy" is a useless goal, not valid for deciding the round

 1. No justification in 1AC

They just make assumptions and hope you won't notice

The Affirmative gives no justification for why the privacy goal matters. They simply assert it by fiat. But why is it bad if privacy is compromised? Why is it so important that it outweighs every other possible consideration in a policy debate? Until they prove these things, it is a sufficient answer to the Affirmative's case to simply reply: SO WHAT? If we vote Negative and privacy is compromised, who cares?

Their "Justifications" are justifications of how their Plan upholds privacy, not justifications of why privacy matters. They have to prove that first. And then they have to justify why it outweighs all other considerations. For example, if a million people starved to death because of their plan, but it protected privacy better than the Status Quo, would that merit an Affirmative ballot? It would if privacy is the only consideration. But that's an insane way to make public policy.

2. Privacy is dead and no one cares

Nobody cares any more about privacy. You already gave it away when you went on Facebook or got a smart phone

Neil Sahota 2020 (IBM Master Inventor, United Nations (UN) Artificial Intelligence (AI) Advisor, Professor at UC Irvine ) 14 Oct 2020 "Privacy Is Dead And Most People Really Don’t Care" https://www.forbes.com/sites/neilsahota/2020/10/14/privacy-is-dead-and-most-people-really-dont-care/?sh=786b31f07b73

Have you read the terms and conditions to use Facebook? Your smart phone? [Most people have not](https://www.npr.org/2014/09/01/345044359/why-do-we-blindly-sign-terms-of-service-agreements), and probably with good reason. They’re hundreds, if not, thousands of pages long. In fact, even contract lawyers with thirty years of experience have struggled in trying to understand these agreements. Deep down, though, each of us knows that we’re signing away our privacy rights to use these platforms and devices. So why do we do it? We don’t truly value privacy as much as we like to believe we do.

Data privacy is pretty much dead

Neil Sahota 2020 (IBM Master Inventor, United Nations (UN) Artificial Intelligence (AI) Advisor, Professor at UC Irvine ) 14 Oct 2020 "Privacy Is Dead And Most People Really Don’t Care" https://www.forbes.com/sites/neilsahota/2020/10/14/privacy-is-dead-and-most-people-really-dont-care/?sh=786b31f07b73

We already live in a world where people are used to sharing everything online. You know those phone phishing scams like the fraudsters pretending to be the IRS? [Young millennials and Generation Z fall victim](https://www.vice.com/en/article/pkedxy/millennials-and-gen-z-get-scammed-more-than-their-grandparents-sorry) to them the most of any generation because they’re used to giving information away. People get important value from these platforms and devices and accept the trade offs for it. Data security is still paramount, but the strong belief for data privacy is pretty much dead.

3. Reverse voting issue

If "privacy" is the voting issue in this round, and the Affirmative never gave any justification prima facie in the 1AC for why privacy matters, then they failed in their duty to present a complete case in their opening speech. If they want that to be a voting issue, then you should immediately do so and vote Negative on it.

4. Counter-Goal

The goal should be: Whoever presents a policy with the least risk of change from the status quo should win the round. Since privacy is a useless goal, as we showed above, a better goal would be to avoid the risks of change while we search for a more worthy goal that would actually justify a change in policy and wouldn't lead to insane conclusions that would justify letting a million people starve.

EXTRA-TOPICALITY

1. Regulations in the Plan go beyond immigration policy

What is Extra-Topicality

It happens when the Affirmative plan does some things in the resolution and adds additional things that go beyond the resolution, then claims advantages or benefits from enacting the untopical parts of their plan. For example, if an Affirmative had a plan to reduce a million visas in the EU next year and launch a manned space mission to Mars. They would have to drop all advantages of space travel from the debate, since those would be coming from an extra-topical mandate.

The Problem: Their Justification 2 on EU citizens gives away the fact that part of their plan is extra-topical

Their evidence from Chris Jones in 2019 says in part QUOTE: "There is already a clear intention to consider bringing other databases and information systems, many of which are principally concerned with EU citizens rather than ‘third-country nationals’, into the scope of the interoperability initiative."

END QUOTE. The fact that their plan is repealing databases that contain information about EU citizens proves it goes beyond immigration. The only way they could achieve any benefits from Justification 2 is by changing policies outside of EU immigration policies, since EU citizens are not immigrating into the EU.

Impact: Drop Justification 2 or else award a Neg ballot

With a resolution this broad, it's abusive to expect Negatives to also research other topics like privacy rights of EU citizens within the EU. At a minimum, this Justification should be dropped from the round. Better yet, a Negative ballot would teach them not to write Plans that don't comply with the resolution and to stop abusing Negative teams they come up against.

HARMS / SIGNIFICANCE

1.  Rights protected outweigh insignificant potential privacy losses

Interop rules have safeguards against privacy loss, and they promote better respect for other human rights

EU Parliament 2019. "Interoperability between EU border and security information systems" June 2019 https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/628267/EPRS\_BRI(2018)628267\_EN.pdf

With regard to fundamental rights, the proposals state that 'the proposed interoperability solutions are complementary components to existing systems' and 'as such, they do not alter the balance already ensured by each of the existing central systems as regards their positive impact on fundamental rights'. The Commission acknowledges that interoperability has the potential to have an 'indirect impact on a number of fundamental rights', such as on the right to respect for private life, the right to dignity and the right to the protection of personal data. However, it also highlights several positive impacts on fundamental rights, such as on preventing identity confusion, detecting missing children, and supporting the implementation of the right to asylum. The proposals are also 'based on the principles of data protection by design and by default' and include 'provisions limiting data processing to what is necessary for the specific purpose’ and granting data access only to those entities that 'need to know'.

2. Privacy violations are compensated under current law

Any violations of personal data trigger a right to compensation for the victim under the 2019 version of the law AFF wants to repeal

Text of Document 32019R0817 2019. (this is the updated and current version of 2017/0351 that is repealed by the AFF plan) EUR-LEX (official repository of EU legislation) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0817

This Regulation should contain clear provisions on liability and the right to compensation for unlawful processing of personal data and for any other act incompatible with it. Such provisions should be without prejudice to the right to compensation from, and liability of the controller or processor under Regulation (EU) 2016/679, Directive (EU) 2016/680 and Regulation (EU) 2018/1725. eu-LISA should be responsible for any damage it causes in its capacity as a data processor where it has not complied with the obligations specifically imposed on it by this Regulation, or where it has acted outside or contrary to lawful instructions of the Member State which is the data controller.

3. Only shows data the investigator was allowed to see

Don't be confused: The new regulations don't allow the investigator to suddenly see all kinds of secret stuff. He can still only see what he was allowed access to under previous rules

Text of Document 32019R0817 2019. (this is the updated and current version of 2017/0351 that is repealed by the AFF plan) EUR-LEX (official repository of EU legislation) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0817

4.   When a query is launched by an ESP user, the EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, the CIR, the MID, the Europol data and the Interpol databases shall in reply to the query provide the data that they hold. Without prejudice to Article 20, the reply provided by the ESP shall indicate to which EU information system or database the data belong. The ESP shall provide no information regarding data in EU information systems, Europol data and the Interpol databases to which the user has no access under the applicable Union and national law.
5.   Any queries of the Interpol databases launched via the ESP shall be performed in such a way that no information shall be revealed to the owner of the Interpol alert.
6.   The ESP shall provide replies to the user as soon as data are available from one of the EU information systems, Europol data or Interpol databases. Those replies shall contain only the data to which the user has access under Union and national law.

4. No one is harmed

No one harmed in the 1AC

The 1AC didn't cite even one example of anyone who had been harmed by the interoperable databases.

Europeans don't feel harmed: 92% of Europeans agree with Negative. Law enforcement should share more data to fight crime & terrorism

Katharina Eisele 2018 (with European Parliamentary Research Service) Feb 2018 Interoperability between EU information systems https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/615649/EPRS\_BRI(2018)615649\_EN.pdf

A Special Eurobarometer survey on Europeans' attitudes towards security shows that the EU's strategy of sharing information at EU level to combat crime and terrorism has widespread public support: 'almost all respondents (92 %) agree that national authorities should share information with the authorities of other Member States to better fight crime and terrorism' (IA, p. 13).

SOLVENCY

1. Reverting to old database system won't solve security problems

The old database system had security holes and data leakages too. Examples from Bulgaria in 2013 and Netherlands in 2011 happened long before the new system was implemented

European Union Agency for Fundamental Rights (also known as FRA) 2017 (agency of the EU conducting research and advocacy for human rights) Fundamental rights and the interoperability of EU information systems: borders and security, May 2017 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/20171019\_interoperability\_eu\_information\_systems\_en.pdf



DISADVANTAGES

1. Terrorism

Link: Without interop, there are delays and inefficiencies when investigating terrorism because authorities don't know in advance which database to look in

Text of Document 32019R0817 2019. (this is the updated and current version of 2017/0351 that is repealed by the AFF plan) EUR-LEX (official repository of EU legislation) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0817

Full access to data contained in the EES, VIS, ETIAS or Eurodac that is necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences, beyond access to identity data or travel document data held in the CIR, should continue to be governed by the applicable legal instruments. The designated authorities responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences and Europol do not know in advance which of the EU information systems contains data of the persons they need to inquire upon. This results in delays and inefficiencies. The end-user authorised by the designated authority should therefore be allowed to see in which of those EU information systems the data corresponding to the result of a query are recorded.

Link: Interop streamlines access to data to speed up prevention, detection or investigation of terrorism

Text of Document 32019R0817 2019. (this is the updated and current version of 2017/0351 that is repealed by the AFF plan) EUR-LEX (official repository of EU legislation) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0817

This Regulation should also introduce a new possibility for streamlined access to data beyond the identity data or travel document data present in the EES, VIS, ETIAS or Eurodac by Member State designated authorities responsible for preventing, detecting or investigating terrorist offences or other serious criminal offences and Europol. Such data may be necessary for the prevention, detection or investigation of terrorist offences or other serious criminal offences in a specific case where there are reasonable grounds to believe that consulting them will contribute to the prevention, detection or investigation of the terrorist offences or other serious criminal offences, in particular where there is a suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence is a person whose data are stored in the EES, VIS, ETIAS or Eurodac.

Link: US Dept of Homeland Security agrees with Negative. Sharing information and enhancing access to it was recommended in their National Strategy to Combat Terrorist Travel in 2018

US Dept of Homeland Security 2018. "National Strategy to Combat Terrorist Travel" Dec 2018 https://www.hsdl.org/?view&did=821737



Impact: Lost lives. Shorter response time is key to saving lives in a crisis

Hajer Faek Kudear AL-Dahash 2017. (PhD candidate; School of the Built Environment, The University of Salford, U.K.) EVALUATION OF DISASTER RESPONSE MANAGEMENT IN IRAQ RESULTING FROM TERRORISM https://usir.salford.ac.uk/44197/1/Final%20thesis%2019th%20Oct%2017.pdf

When examining disaster response, time is one of the essential elements that should be noted and considered (Miller, 2007). To limit damage to people, property and environment, dire consequences, that are typically delivered from complex disaster problems, must be solved in a very short amount of time (Torma-Krajewski & Powers, 2010). Because in the domain of disaster response, minutes of delay can cost lives and property, so speed is typically essential.

2. Lost human rights and benefits

Interop upholds a number of rights better than without it. And it helps solve human trafficking of children

European Union Agency for Fundamental Rights 2017 (agency of the EU conducting research and advocacy for human rights) Fundamental rights and the interoperability of EU information systems: borders and security, May 2017 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/20171019\_interoperability\_eu\_information\_systems\_en.pdf

Interoperability can support the detection of missing children or children subject to trafficking in human beings, and facilitate a targeted response. This requires the systematic recording of missing children in SIS II, and an additional focus on child protection in the indi­vidual IT systems. Interoperability can also contrib­ute to respect for the principle of non-*refoulement* by ensuring that the status as an applicant for international protection is also visible when consulting other infor­mation systems. Risks for discriminatory profiling may be reduced if a combination of non-sensitive criteria is used instead of relying on a limited number of sensi­tive categories.

3. Increased illegal immigration

Link: EU Interop reduces illegal immigration

European Council 2020 (part of the EU government) IT systems in the area of freedom, security and justice, last updated 14 Dec 2020 https://www.consilium.europa.eu/en/policies/it-systems-in-the-area-of-freedom-security-and-justice/



Impact: Lost jobs from illegal immigration

Dr. Pia Orrenius and Dr. Madeline Zavodny 2016 (Pia M. Orrenius, holds a PhD in Economics from the University of California at Los Angeles. She is Vice President and Senior Economist at the Federal Reserve Bank of Dallas. Madeline Zavodny received a PhD in Economics from the Massachusetts Institute of Technology. She is a Professor of Economics at Agnes Scott College, Department of Economics & Business Management) January 2016 “Irregular Immigration in the European Union” <https://www.eapmigrationpanel.org/sites/default/files/2016_2_epa_eng_1.pdf>

Few studies of the labor market effects of immigration look specifically at unauthorized immigrants because of the difficulty of determining immigrants’ legal status. Evidence suggests that unauthorized immigrants typically earn less than natives or legal immigrants. In Italy, for example, irregular immigrants earn about 8 percent less than comparable legal immigrants; in Spain, 12 percent less (Baldacci, Inglese, and Strozza, 1999; Connor and Massey, 2010). Research shows that immigrants working illegally in the shadow economy in Italy reduce employment of legal labor there (Venturini, 1999). However, natives working illegally (off the books) have a more adverse effect on legal employment there than immigrants working illegally.

Impact: Black market work causes economic and social harm

Report by Solidarite and Diesis 2010 (With the financial support of the European Community Programme for Employment and Social Solidarity PROGRESS (2007-2013)) “THE ILLEGAL WORK OF MIGRANTS IN THE EUROPEAN UNION” (no month given in the publication) <https://www.pourlasolidarite.eu/sites/default/files/publications/files/report_illegal_work_of_migrants_in_the_eu_0.pdf>

The development of an informal economy weakens the European social model. Since 2007, the European social affair Commissioner, Vladimar Spidla, has assessed the black market as being „extremely harmful to our economies. The fact that neither the employer, nor the employee pays taxes strongly weakens social security systems, which has already been put to the test by the economic crisis and Europe’s aging population. If we do nothing, these practices will lead to a form of social dumping, which means that salaries in some sectors will become very low for companies to stay competitive’ he underlines.

Link: Illegal immigrants destroy native jobs in irregular sectors

Prof. Alessandra Venturini 2004 (Associate Professor, Dept of Economics, University of Turin, Italy) January/February 2004 “Do Illegal Migrants Compete with National Workers?” <https://www.intereconomics.eu/pdf-download/year/2004/number/1/article/the-illegal-employment-of-foreigners-in-europe.html>

In their excellent field work in Northern Greece, Lianos, Sarris and Katseli estimated by interviews the gross substitution of native workers by foreigners, i.e. how many jobs previously done by Greeks are now done by foreigners. The gross substitution rate was very high: 12% with reference to regular immigrants and 21% with reference to irregular immigrants, but taking into account the reduced willingness of native workers to do certain kinds of jobs and tasks, the net substitution rate is reduced to 0.5% for regular and 5.8% for irregular labour. These results suggest that in each labour market immigrants play a competitive role, but in the irregular labour market their role is much larger, as is to be expected from neoclassical theory, because the effect is larger where the market is more flexible. In addition these results suggest that irregular labour damages native workers more than regular labour and thus it is better to legalise immigrants.