Data Havens, or Privacy Sans Frontières? A Study of International Personal Data Transfers

Reuben Binns, Dr. David Millard, Dr. Lisa Harris
Web Science Doctoral Training Centre
University of Southampton
Southampton, UK
{rb5g11,D.E.Millard,l.j.harris}@soton.ac.uk

ABSTRACT

The web routinely spreads personal data from one jurisdiction to another, where levels of legal protection over such data vary. This raises the potential for some jurisdictions to become 'data havens' specialising in either strong protection of data, or allowing its unrestricted use [5],[3]. In order to promote interoperability and harmonisation, some jurisdictions with similar levels of protection may approve each others data protection regimes, lifting restrictions on international transfers[4].

This article presents a quantitative analysis of over 16,000 international data transfer arrangements made by UK organisations in 2013. Our findings support the hypothesis that one jurisdictions' approval of another's data protection regime is associated with more data transfer arrangements between them. We conclude with implications for the future of cross-border data transfers and the prospect of 'personal data havens'.

Categories and Subject Descriptors

K.4.1 [**Public Policy Issues**]: Regulation, Transborder data flow, Privacy

General Terms

Economics, Legal Aspects

Keywords

International Data Transfers; Data Protection; Data Havens.

1. INTRODUCTION

While the web is global, most of the laws which govern it are national or supranational. In the realm of data protection, this means different jurisdictions offer different types and degrees of privacy protection and rules for organisations who use personal data. To complicate matters, the individual whom the data is about, the organisation responsible for it, and the server on which it is stored may each be located in different jurisdictions.

Some providers of web services appear to be attempting to exploit this situation, using their location in a jurisdiction with strong data privacy laws to gain a competitive advantage. In August 2013, in the wake of controversy over U.S. government surveillance activity, three of Germany's largest email providers jointly launched a new service called 'Email Made in Germany' which promotes itself as protecting the inbox in accordance with German law [2]. If choice of jurisdiction becomes an important product differentiator for privacy-conscious consumers, some states may seek to boost their domestic web service industry by ensuring high privacy protections.

At the same time, in order to promote a cross-border digital market, some states have sought to harmonise their respective data protection regimes and lift restrictions on the flow of personal data between them[1]. For instance, cross-border transfers within the European Economic Area do not require additional approval. For 'third country' (non-EEA) jurisdictions, the European Commission issues decisions on the adequacy of their data protection regimes. Transfers of data to organisations located in 'adequate' jurisdictions involve less onerous responsibilities for the transferring parties [2]. If inter-jurisdictional harmonisation and/or approval is worthwhile, it ought to go hand-in-hand with data transfers between those jurisdictions. In this study we test the hypothesis that EU regulatory approval of a third country's regime is associated with more data transfer arrangements from the UK to that country.

2. DATA SOURCE AND EXTRACTION

The data source is the UK Information Commissioner's Office's register of data controllers (February 2013), which features over 350,000 UK organisations. The UK Data Protection Act states that data controllers must contact their national supervisory authority, notifying them (amongst other things) of any arrangements for transfers of personal data to third countries (Section 16, 1f, Data Protection Act 1998).

[1]We use the UK Data Protection Act (DPA) definition of personal data: 'data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller' (DPA 1998, s.1)

[2]Countries with adequacy status include Andorra, Argentina, Australia, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay, and the United States [1]

WebSci'14, June 23–26, 2014, Bloomington, IN, USA.
ACM 978-1-4503-2622-3/14/06.
http://dx.doi.org/10.1145/2615569.2615650.

Country	Transfers	Country	Transfers
USA	8060	Singapore	334
India	1627	**New Zealand**	322
Canada	1064	**Isle of Man**	293
Australia	1042	Philippines	168
Guernsey	879	Malaysia	129
Switzerland	575	Dubai	117
Japan	551	**Israel**	117
South Africa	448	Turkey	80
Hong Kong	370	Brazil	63
Jersey	353	Pakistan	63

Table 1: The 20 most common destinations for international data transfers from the UK. Jurisdictions whose data protection regimes have been approved by the European Commission are highlighted in bold.

The register is made available as XML. We first parsed the data using SAX [3], then restructured it as an SQL database which was queried to extract relevant portions of the data for further analysis.

3. RESULTS

Most instances of data collection described in the register (90.1%) claimed not to transfer data outside the European Economic Area (EEA). 8.6% were listed as 'Worldwide', with no further specificity about locations. The remaining 1.3% (16,906) reported specific jurisdictions to which the data was transferred.

We separated the recipient countries into two populations; those who have been approved by the EC as 'adequate' in their data protection regime, and those who have not. 'Adequate' countries were found to be the destination of international data transfers more often (a mean average of 961 against the general average of 457). We repeated this after excluding the USA from the results, as it accounts for nearly half of all specified transfer arrangements and therefore may be considered an outlier. Also, unlike other jurisdictions listed as 'adequate' by the Commission, the US is considered adequate for transfers only if the recipient organisation has signed up to the 'Safe Harbour' programme [4]. We still found a higher average transfer frequency for countries with approved adequacy status (463) than the general case (252).

Finally, in order to show how these numbers relate to general business relations between jurisdictions, we also calculated a new score for each country. This is expressed by the ratio of the value of the UK export market for that country (in $million), to its total number of data transfer arrangements[5]. The average score for adequate countries was 6:1, compared to 47:1 for non-adequate countries, i.e. the former had more transfer arrangements in relation to their general export market value. This indicates that even adjusting for existing trade relations, 'adequate' countries have a greater number of transfer arrangements.

[3]www.saxproject.org

[4]http://export.gov/safeharbor/

[5]Where data was available, based on historical figures released by the UK Office for National Statistics on UK trade, available at http://www.ons.gov.uk/ons/rel/uktrade/uk-trade/february-2014/index.html

4. DISCUSSION

These preliminary results paint a picture of the flow of personal data from the UK to countries outside Europe. Further research will be needed to establish a robust causal relationship between adequacy status and international transfers, and if so, the direction of causation. Further longitudinal analysis could provide evidence one way or the other by comparing the change in frequency of transfers to a jurisdiction before and after the EC issues a positive adequacy decision. Only two countries (New Zealand and Uruguay) were given this status during the time period for which data is available (2011-2013), for which the change in transfer volume was negligible (+2.5% and 0 respectively).

5. CONCLUSIONS

Cross-border personal data flow is much higher between jurisdictions with harmonised or 'approved' privacy laws, evidenced by the higher portion of transfers from the UK which do not leave the EEA, and the higher average number of recipients in non-EEA countries whose levels of protection have been deemed adequate by the EC. Harmonisation and its effect on international transfers has implications for those governments attempting to create 'data havens' with strong privacy protections (and for the emerging web companies who seek to benefit from locating themselves within them). Strong privacy laws may be needed in order to gain another state's approval and therefore access to foreign privacy-conscious consumer markets.

But states also have an incentive to be selective with their approvals; the privacy credentials of a given jurisdiction depend partly on the privacy credentials of *other* jurisdictions it allows personal data to be transferred to without restriction. If strong privacy laws are to become a selling point for domestic web services, governments may also need to ensure that those laws only permit personal data to be transferred to third countries if they can ensure equal levels of protection.

6. ACKNOWLEDGMENTS

This research was funded by the RCUK Digital Economy Programme, EP/G036926/1.

7. REFERENCES

[1] E. Commission. Commission decisions on the adequacy of the protection of personal data in third countries.

[2] F. R. Elizabeth Dwoskin. Nsa internet spying sparks race to create offshore havens for data privacy.

[3] J. N. Geltzer. New pirates of the caribbean: How data havens can provide safe harbors on the internet beyond governmental reach, the. *Sw. JL & Trade Am.*, 10:433, 2003.

[4] C. Kuner. The european commission's proposed data protection regulation: A copernican revolution in european data protection law. *Privacy and Security Law Report*, 11:1–15, 2012.

[5] M. U. Porat. Global implications of the information society. *Journal of Communication*, 28(1):70–80, 1978.