The limits of the US Judicial Redress Act

Edward Hasbrouck analyses the new law which provides limited privacy rights for Europeans – and only for personal data processed by the US federal government.

European Union Commissioner for Justice, Věra Jourová, described the US Judicial Redress Act[1] signed into law by President Obama on 24 February 2016 as, "a historic achievement [that] will ensure that all EU citizens have the right to enforce data protection rights in US courts…. The entry into force of the Judicial Redress Act will pave the way for the signature of the EU-US Data Protection Umbrella Agreement."

But the limitations and exceptions in the Judicial Redress Act, and the experience of US citizens who have sought redress in US courts for privacy violations, cast doubt on whether this law will really "ensure that all EU citizens have the right to enforce data protection rights in US courts." There are likely to be few real-world cases in which the Judicial Redress Act will provide enforceable legal rights to citizens or residents of the EU, or anywhere else.

The Judicial Redress Act gives some foreign citizens some of the rights that US citizens currently have, with respect to some of the uses and misuses by the US government of their personal information. But in no case will any foreigner have more rights under the Judicial Redress Act than US citizens have under the Privacy Act[2].

Serious scrutiny of the terms of the Privacy Act, and of the history of attempts by US citizens to use the Privacy Act to protect ourselves against misuse of our personal information by the US government, has been largely absent from the debate about the Judicial Redress Act. But from our experience as the plaintiff in one of the key test cases in which US citizens have attempted to assert Privacy Act claims against the US government[3], we have learned an important lesson that Europeans need to know: the Privacy Act is so limited and riddled with exceptions that it is almost worthless.

All of the limitations and exceptions that always rendered the "protection" of the Privacy Act inadequate — even for US citizens — will continue to render the protection of the Judicial Redress Act inadequate for foreigners, in all of the same ways, and in additional ones.[4]

What are these exceptions and limitations? In order to make sense out of the Judicial Redress Act, it's essential to understand the exemptions in the Privacy Act, as courts have interpreted them.[5]

Federal agencies can exempt themselves from almost all of the requirements of the Privacy Act with respect to "investigatory material compiled for law enforcement purposes," a catch-all category that has been applied to records of dragnet surveillance and other information compiled and used for "pre-crime" profiling, even when the data subjects have never been accused or suspected of any crime. All an agency has to do to opt-out is to publish a notice in the Federal Register that a particular system of records has been declared exempt by the agency that maintains the records. An agency can wait to promulgate such a notice until after it receives a request for access to records, a request for an accounting of disclosures, or a request for correction of records.

Under the interpretation of the Privacy Act adopted by the US government and upheld by a Federal District Court – the court when it was challenged for the first time in our litigation, additional Privacy Act exemptions can be promulgated at any time in the future, and applied even to requests that had already been made. In light of this ruling, nobody can rely on any "rights" under the Privacy Act that could be retroactively revoked at any time. Once such exemptions are promulgated, individuals – even US citizens – have no right under US law to see what records are being kept about them, and no right to know how or according to what algorithms data about themselves is mined, processed, or otherwise used. No logs need be kept of who accesses records, or to whom they are disclosed.

The rules published by the US Department of Homeland Security to exempt records in the DHS Automated Targeting System (including commercial data about customers and other individuals obtained from private companies) from the requirements of the Privacy Act are typical of the exemptions that have been promulgated for numerous other systems of Federal records about individuals:

The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (e)(5), and (8); (f); and (g) pursuant to 5 U.S.C. 552a(j)(2).[6]

To understand what an exemption rule like this this means, one has to read the clauses of the Privacy Act referred to in the exemption rules. These DHS records have been exempted by the DHS from each of the following requirements of the Privacy Act:

- The right of a data subject to access records about herself.
- The right of a data subject to receive, on request, an accounting of disclosures of her personal data to other agencies or third parties.
- The prohibition on maintaining records about individuals that are not relevant and necessary to accomplish a legal purpose of the agency.
- The requirement to maintain records which are used in making determinations about individuals "with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual."
- The requirement to collect personal information "to the greatest extent

practicable" directly from the data subject rather than from third parties.
- The requirement to notify data subjects of what information about them is being collected, and from whom it is being collected.
- The right of a data subject to to dispute, amend, or correct records about herself.
- The right of a data subject to add a notice of disputed data in records about herself, and to have that notice included whenever the disputed portion of the record is disclosed to a third party.

It's not just the DHS that has opted out of the Privacy Act. The NSA has similarly exempted its surveillance records from the Privacy Act: "The problem is that Europeans are likely to notice that the Privacy Act provides no meaningful redress to targets of NSA surveillance. Agencies can exempt themselves from the Privacy Act's access and redress provisions on grounds of national security. U.S.C. § 552a(k). The NSA has taken full advantage of this section. 32 C.F.R. § 322.7(a)."[7]

Once an agency has published a notice exempting a system of records from these requirements of the Privacy Act, it is completely legal (or at least, it is not a violation of the Privacy Act for which a US citizen or anyone else can sue the agency) for the agency to fill that database with secret information about individuals, collected from undisclosed third parties, that it knows is likely to be inaccurate, outdated, incomplete, and irrelevant to any lawful purpose. The agency can withhold all of this information from the data subject, and secretly disclose any or all of it to any other government agency or third party anywhere in the world. Any disclosure of exempt records that an agency chooses to make is "discretionary" and not subject to judicial review.

For the reasons discussed above, the Privacy Act gives US citizens inadequate legal protection. But even with the Judicial Redress Act, Europeans and other foreigners (even citizens of the most preferred foreign nations) will continue to have even less protection and fewer rights than US citizens, in at least two important ways that have not been widely noted.

First, even with respect to records that have not been exempted from the Privacy Act, the Judicial Redress Act gives foreign citizens the right to sue to enforce only some, but not all, of the rights that US citizens can sue to enforce under the Privacy Act. Specifically, foreign citizens can bring lawsuits in US courts only for violations of "section 552a(g)(1)(D) of title 5, United States Code" or "subparagraphs (A) and (B) of section 552a(g)(1) of title 5, United States Code" but not under any of the other provisions of the Privacy Act. These sections cover refusal by a Federal agency to comply with a subject access request or request for amendment of a record, but notably exclude lawsuits by foreigners for violations of subparagraph (C), which allows a US citizen to sue an agency that "fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relation to … the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual."

The exclusion of subparagraph (C) from the causes of action allowed by the Judicial Redress Act, while including subparagraphs (A), (B), and (D), appears deliberately crafted to preclude challenges by foreigners to the use of unreliable and irrelevant third-party data in profiling, risk assessments, and similar algorithmic processing and scoring systems.

Second, records are "covered" by the Judicial Redress Act only if they have been transferred:

(a) by a public authority of, or private entity within, a … covered country; and
(b) to a designated Federal agency or component for purposes of preventing, investigating, detecting, or prosecuting criminal offenses.

This excludes two key categories of records: records maintained for

'SAFE HARBOR' REPLACEMENT : EUROPEANS' COMPLAINTS WILL TAKE PRIORITY OVER AMERICANS'

European and US negotiators have reached agreement on a plan for transfer of personal information across the Atlantic that continues to provide more protection by US agencies to Europeans than Americans.

Because of a decision by the European Court of Justice last October that invalidated the "Safe Harbor" scheme developed by the US Department of Commerce, a new agreement was necessary to continue permission for international companies to remove personal data from Europe

The European Commission on Feb. 2 announced agreement on a new "EU-US Privacy Shield," with only a few details:

• The US will establish an ombudsman in the Department of State to address complaints related to US intelligence authorities' access to data about Europeans. American citizens and residents have no such redress.

• The US Office of National Intelligence has made binding commitments that US access to Europeans' data for national security purposes will have "clear limitations, safeguards and oversight mechanisms" limiting the access to what is "necessary and proportionate." The US has also agreed to an annual review of these commitments. American citizens have no such assurances.

• The US Department of Commerce will monitor companies to ensure that they publish their privacy commitments, which then become enforceable by the Federal Trade Commission, similar to the previous Safe Harbor Framework. But the privacy policies need not provide any protections for Americans.

• European Union individuals will have access to free alternative dispute resolution mechanisms. Americans will not benefit from this.

• European regulators will have a formal channel to refer complaints to the US Department of Commerce and the FTC. Complaints from Europe will need to be resolved by stated deadlines, meaning that they will have priority over complaints by Americans, where there are no required deadlines.

• American companies participating in the new EU-US Privacy Shield will need to commit to "robust" obligations, including submission to European jurisdiction when transferring employee data.

In exchange the Europeans will issue an "adequacy decision' by this spring asserting that US privacy protections are "adequate" for transferring data from Europe to here. Presumably the agreement binds only the Obama Administration, not its successors.

By Robert Ellis Smith.

Reproduced with permission from Privacy Journal, February 2016 p.3 www.privacyjournal.net/

purposes other than enforcement of criminal laws, and records transferred from the EU to the US government by way of commercial intermediaries in the US (or in third countries that are not covered by the Judicial Redress Act).

Many US laws and regulations are enforced by civil, rather than criminal, sanctions. Records maintained by the US government for civil enforcement purposes are completely exempt from the Judicial Redress Act, as are all records maintained for any purpose except criminal law enforcement.

Records maintained for criminal law enforcement purposes can be (and almost always have been) exempted from the Privacy Act. Records maintained for any other purpose are exempt from the Judicial Redress Act. The result is that hardly any records will fall through the cracks between the exemptions in these two laws, and provide a basis for a lawsuit by a foreign citizen.

Even if either or both the Privacy Act and/or the Judicial Redress Act were amended to remove these exemptions, the limitation of the Judicial Redress Act to records transferred directly from an entity in the EU to the US government would leave a huge loophole, of exactly the sort the US has exploited in the past to intercept personal and commercial information about financial transfers between European banks from servers of SWIFT in the US, information about electronic communications between other countries from intermediaries in the US through which messages were routed, and airline reservation data ("passenger name records") collected by European airlines, travel agents, and tour operators stored with computerized reservation systems in the US.

The Privacy Act provides inadequate data protection for US citizens, and the Judicial Redress Act would provide even more inadequate protection for non-US citizens. Neither of these laws provides any basis for a finding that anyone's rights are adequately protected in the US, or for approval of the proposed "Privacy Shield" or the proposed EU-US "umbrella agreement" on data transfers.

AUTHOR

Edward Hasbrouck is consultant to the Identity Project – PapersPlease.org.
Email: edward@hasbrouck.org

REFERENCES

1 H.R. 1428, Judicial Redress Act of 2015, www.congress.gov/bill/114th-congress/house-bill/1428
2 5 U.S.C. § 552a
3 *Hasbrouck v. US Customs and Border Protection*, Case C 10-03793 RS, US District Court, Northern District of California. See case documents and discussion at https://papersplease.org/wp/hasbrouck-v-cbp/
4 See Robert Gelmann, 'Foreigners' privacy rights in the US: Little more than a gesture,' *PL&B International*, October 2014.
5 See the round-up of case law on Privacy Act exemptions compiled by the US Department of Justice at www.justice.gov/opcl/ten-exemptions
6 'Privacy Act of 1974: Implementation of Exemptions,' 75 Federal Register 5487-5491, 3 February 2010, www.gpo.gov/fdsys/pkg/FR-2010-02-03/html/2010-2201.htm
7 Timothy Edgar, 'Redress for NSA Surveillance: The Devil Is in the Details', Lawfare blog, 19 October 2015, www.lawfareblog.com/redress-nsa-surveillance-devil-details

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

German DPA takes action against Safe Harbor firms

Hamburg's DPA is investigating and prepared to issue fines. By **Sascha Kuhn**.

At the end of February, Hamburg's Data Protection Commissioner, Johannes Casper, instituted three proceedings, against subsidiaries of US companies suspected of unlawful transfer of personal data to the United States. Upon completion of the hearings and the proceedings the companies could face fines of up to €300,000 each. The companies had continued using the Safe Harbor Principles of the European Commission (EC) as a legal basis for transferring personal data to their respective parent companies in the US, although this legal

Continued on p.3

EDPS nurtures consumer and DP/competition law cooperation

Giovanni Buttarelli says that closer cooperation between competition, consumer protection and data protection authorities has started. **Laura Linkomies** reports.

Speaking at PL&B's Roundtable in Brussels on 9 March, **Giovanni Buttarelli**, European Data Protection Supervisor (EDPS), said that he is actively working on the dilemmas emerging at the threshold of data protection and antitrust law, complemented by international trade agreements. He said that while it was previously

Continued on p.4

Issue 140 **April 2016**

INTERNATIONAL report

ISSUE NO 140 APRIL 2016

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

SUB EDITOR
Tom Cooper

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
Glenn Daif-Burns
glenn.daif-burns@privacylaws.com

CONTRIBUTORS
Hui-ling Chen
Winkler Partners, Taiwan

Lorna Cropper and Kate Pickering
Fieldfisher LLP, UK

Sebastian Golla
Germany

Edward Hasbrouck
Identity Project, US

Kuan Hon
Queen Mary University of London, UK

Sachsa Kuhn
Simmons & Simmons LLP, Germany

Blair Stewart
Privacy Commission, New Zealand

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Safe Harbor no longer safe

A German Land (city state) Data Protection Authority has taken the lead in starting enforcement against three Safe Harbor companies (p.1). Hamburg's DP Commissioner, Dr Johannes Caspar, has not yet declared which firms are involved, but has said that they are large international companies, which should have the legal knowledge and resources to deal with the issue. Caspar is now consulting the affected companies on whether they wish to exercise their right to a hearing. In an interview with *Der Spiegel Online*, the Commissioner said that "There are probably companies that do not seem to take the situations seriously or are willing to accept the risk of fines." Meanwhile, the proposed replacement, the EU-US Privacy Shield, has both supporters and critics (p.6).

On p.23, Stewart Dresner provides an update on the Belgian Facebook case. As a result of many years of close contact from organising conferences and roundtables with them, we are very fortunate to have access to DPAs themselves and learn directly from their staff too. This was the case in Brussels in March, when we organised a Roundtable with the European Data Protection Supervisor, Giovanni Buttarelli. The EDPS is keen to bring data protection, competition and consumer law issues closer together, and is preparing for its important future role under the GDPR as Secretariat to the European Data Protection Board. Read highlights of this meeting from p.1. In addition, the speakers' slides are available to subscribers via *PL&B's* website (p.6).

The EU General Data Protection Regulation continues to be a concern to companies. Data processors will face new responsibilities and will be liable for breaches of the Regulation (p.29). Those using cloud computing need to understand the implications of the Regulation's extra-territorial scope (p.25). But the Regulation also has an influence outside Europe – read on pp.7-9 how the concept of data portability has crept into the law of the Philippines.

The UN Special Rapporteur on Privacy, Professor Joseph Cannataci, has delivered his first Report to the UN Human Rights Council, (pp.10-12) saying he wants to increase awareness and engagement, but what can be achieved without adequate resources? In India, the government is advancing with its plans to introduce a nationwide ID system. There are concerns over data matching which will become easier but remain unregulated (pp.18-20).

Finally, our correspondents in Turkey tell us that the data protection law has been accepted by the Parliament, but the law has not yet been published in its final form in the Official Gazette. As it was not possible to obtain the final version of the law before publication, we will report on this new law in our next issue.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 100+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
You will be sent the PDF version of the new issue on the day of publication. You will also be able to access the issue via the website. You may choose to receive one printed copy of each Report.

3. E-Mail Updates
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Chief Privacy Officer, BT Retail, UK**"

Subscription Fees

Single User Access

International Edition **£500 + VAT***

UK Edition **£400 + VAT***

UK & International Combined Edition **£800 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-4 or 5-25 users – see website for details.

Subscription Discounts

Special charity and academic rate:
50% discount on all prices. Use HPSUB when subscribing.

Number of years:
2 (10% discount) or 3 (15% discount) year subscriptions.

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.
www.privacylaws.com/UK