Universiteit Utrecht

Data Protection, Profiling and Anti-Fraud Systems

A Comparative State Practice Report

***

31 March 2016

Authors:

Steven van Dalen
Alexander Gilder
Eric Hooydonk
Marc Ponsen

Supervisors:

Dr Brianne McGonigle Leyh
Mistale Taylor LLM

Executive Summary

This memorandum focuses on the jurisdictions of the United Kingdom (UK), Germany and the United States (US) to provide contrasting examples of data protection principles and of anti-fraud systems similar to SyRI.

Systems with similar or resembling objectives as SyRI, namely the prevention of social welfare fraud or medical fraud, were analysed with regard to the UK and the US. Both jurisdictions' national justifications for use of the systems were always the combatting and prevention of fraud and meeting the public demand to prevent crime and misuse of public goods. This is identical to the justifications for the use of SyRI in the Netherlands. Within the parameters of the research, no system in Germany was found which shares data between governmental institutions with the purpose of the prevention of fraud. The legal framework regarding data protection is however quite extensive and has been analysed in order to provide for a comparison to some of the principles governing SyRI.

Regarding the UK and the US the risks and threats were examined for each jurisdiction's respective systems. This provided conclusions on the merits and shortfalls of systems similar to SyRI and of systems that share different types of data but still have similar risks to that of SyRI. These risks include:

- violations of the right to privacy;
- the danger of stigmatising citizens making social welfare claims and the related potential of profiling specific social groups as such possibly leading to discrimination or unequal treatment;
- infringements of confidentiality of personal data;
- limited protection of data subjects by the law, use of incorrect or biased data and other risks related to the quality of the data;
- a lack of transparency of the data processing measures; and
- a lack of oversight and accountability;
- a lack of redress.

Table of Contents

Glossary of Defined Terms **5**
Glossary of Abbreviations **6**
1. Introduction **7**
2. United Kingdom **8**
2.1 Legal framework 8
2.2 Overview applicable data sharing or profiling systems 8
2.3 Justifications for the use of the systems 10
2.4 Risks and threats 11
2.5 Interim conclusion 12
3. Germany **13**
3.1 Legal framework 13
3.3 Overview applicable data sharing or profiling systems 13
3.3 Risks and threats 13
3.4 Interim conclusion 15
4. United States **16**
4.1 Legal framework 16
4.2 Overview applicable data sharing or profiling systems 17
4.3 Justifications for the use of the systems 19
4.4 Merits of the justifications 20
4.5 Risks and threats 20
4.6 Interim conclusion 22
5. Conclusion **23**

Glossary of Defined Terms

'Controller'	'natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law'[1]
'Personal data'	'any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'[2]
'Processing' or 'processing of personal data'	'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'[3]

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive or DPD), Art. 2(d). Available at: <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046>, last accessed 18 March 2016.

[2] DPD, Art. 2(a)

[3] DPD, Art. 2(b)

Glossary of Abbreviations

AFI	Analytical Framework for Intelligence
ATS	Automated Targeting System
CBP	Custom and Border Protection
CoE	Council of Europe
CMS	Center for Medicare and Medicaid Services
DPA	Data Protection Act 1998
DPD	Data Protection Directive
DWP	Department for Work and Pensions
ECHR	Convention for the Protection of Human Rights and Fundamental Freedoms
EU	European Union
FALCON-DARTTS	FACLON Data Analysis and Research for Trade and Transparency System
FALCON-SA	FALCON Search and Analysis System
FBI	Federal Bureau of Investigation
FDPA	Federal Data Protection Act
HRA	Human Rights Act 1998
ICE	Immigration and Customs Enforcement
NGO	Non-governmental organisation
SSFA	Social Security Fraud Act 2001
SyRI	System Risk Indication
UK	United Kingdom of Great Britain and Northern Ireland
US	United States of America

1. Introduction

This memorandum focuses on three different jurisdictions to provide contrasting examples similar to SyRI. It includes the United Kingdom (UK), Germany and the United States (US). Firstly, this memorandum examines the legal framework for data protection and data sharing systems for each jurisdiction. Secondly, every section outlines data processing systems discovered in the research. For the UK and US this includes systems with similar fraud preventing objectives to that of SyRI, whereas for Germany, no similar system was found. Thirdly, the memorandum shows the jurisdiction's national justifications for use of the systems, to demonstrate the range of objectives different States seek to complete. Fourthly, each section identifies the risks and threats for each jurisdiction's respective systems. This process provides conclusions on the merits and shortfalls of systems akin to SyRI and systems that share different types of data but still have similar risks to that of SyRI.

The research seeks to answer the question: 'What data sharing and profiling systems exist in influential jurisdictions and what risks exist in relation to their use?' The legal systems selected for research are influential and different in structure. The UK is purely common law, the US is a variant of common law with elements of civil law and Germany is a civil law system. The analysis of those three systems provided for examination of legal frameworks with regards to data processing. The frameworks are in fact similar to the Netherlands, and in the cases of the UK and US include systems currently in use that are similar to SyRI. For both EU countries, the comparison is useful due to the differing state implementation of EU law. That different implementation can result in similar systems with a slightly altered domestic legal framework within which they operate. The US provides for a contrasting example where a social welfare fraud detection system exists but with another applicable data protection regime.

The UK has an express legal framework for data sharing in relation to social welfare fraud in the form of the Social Security Fraud Act 2001 and Welfare Reform Act 2012. Further, the UK operates the General Matching Service under the Department of Work and Pensions with the goal of preventing fraud and saving public money. The US has a multitude of systems, five of which are detailed in the memorandum. Most similar to SyRI is the Medicare-Medicaid Data Match Program which shares and processes data with the purpose of preventing healthcare fraud. The research performed did not find any governmental data sharing systems in Germany. However, the legal framework for data protection and sharing in Germany is detailed. Finally, no case law was found related to data processing to combat fraud. An explanation for this is that intervention teams will use risk notifications as a starting point for further investigation. The initial notification will therefore not be used as evidence and will thus seldom be scrutinised.

2. United Kingdom

This jurisdiction report outlines UK law, including specific social security fraud legislation. It next discusses a number of systems mainly used by the Department for Work and Pensions (DWP) in combating fraud. Furthermore, it outlines the justifications of the government for the use of the systems. Finally, it identifies the risks posed by the use of the systems.

2.1 Legal framework

Data is protected in the UK under the Data Protection Act 1998 (DPA) and the Human Rights Act 1998 (HRA). The HRA gives effect to the European Convention on Human Rights (ECHR) in domestic law including Article 8 and the right to a private and family life. The DPA provides the framework for the handling, storage and processing of data and personal information by all persons and bodies. The DPA was introduced to codify in UK law the EU's 1995 Data Protection Directive. However, the DPA has exclusions of application of the Act's principle of fair processing of data when being used for crime or taxation purposes (s.29) and health, education and social work (s.30). For instance, Section 30 includes the right of government departments and local authorities to exempt provisions when processing personal data for social work.

The Social Security Fraud Act 2001 (SSFA) allows for 'authorised officers' to request information from a variety of sources including insurance companies, credit companies and banks, if the officer reasonably believes the claimant of social welfare is committing or intending to commit an offence, for instance, fraud.[4] One author regards this as a wide power due to the words 'intending to commit' and 'reasonable suspicion'.[5] The author says, 'the government has never viewed the data matching provisions of the SSFA 2001 as compromising data protection principles'.[6]

Another example of data sharing in the law can be found at s.127-134 of the Welfare Reform Act 2012. Section 128 includes data sharing with the Director of Public Prosecutions for the purposes of instituting criminal proceedings relating to social security matters, such as welfare fraud.

2.2 Overview applicable data sharing or profiling systems

The UK has extensive intergovernmental data sharing and links between databases.[7] The Department for Business Enterprise and Regulatory Reform may carry out covert and non-intrusive surveillance to uncover fraud.[8] The DWP is a large data processer for social welfare

[4] Social Security Fraud Act 2001 s.1(2).
[5] McKeever G, 'Balancing rights and responsibilities: the case of social security fraud' [2009] J.S.S.L. 16(3) p.148.
[6] McKeever G, 'Balancing rights and responsibilities: the case of social security fraud' [2009] J.S.S.L. 16(3) p.149.
[7] Select Committee on the Constitution, 'Surveillance: Citizens and the State' (2nd Report of 2008-09, 6 February 2009, HL Paper 18-I) [87].
[8] Select Committee on the Constitution, 'Surveillance: Citizens and the State' (2nd Report of 2008-09, 6 February 2009, HL Paper 18-I) [88].

and coordinates data sharing with a multitude of sources 'to prevent and detect fraudulent claims, for example by matching death information from the General Register Office with customer records.'[9] The DWP says its work is reactive rather than proactive and answers data matching requests from governmental agencies.[10] The Data Matching Service, in 2008, was described to run '148 rules' to match data across sources such as DWP benefits, Housing and Council Tax, Prisoner data, Royal Mail, NHS Prescriptions, Students Loan Company, Passport Service and the Electoral Register.[11] The service trialled matching with credit reference agencies to further detect social welfare fraud and a voice risk analysis system to identify when a caller's voice was stressed that could indicate lying about social welfare circumstances.[12]

A separate programme in 2012-13 sought to match data from the DWP and the Electoral Register to confirm identities and residences for reform of the register.[13] A document details the six stage matching process that includes matching unique property numbers, postcodes and the last names of residents with DWP data.[14]

In 2013, a freedom of information request was made concerning the DWP General Matching Service. The response detailed that the General Service, Referral Management System and the Fraud Referral and Intervention Management System can identify cases of fraud. The DWP attached the Data Matching Guidance for employees using the systems, which is a comprehensive user manual for the computer software that matches data.[15] A second attachment detailed how departments must deal with referrals of a risk of fraud.[16] For example, one risk that the system can flag is where parents claim social welfare for their children when they are no longer in the household. The DWP must take action to verify if the children have in fact moved. The system is able to match across Carers Allowance, Child

[9] Select Committee on the Constitution, 'Surveillance: Citizens and the State' (2nd Report of 2008-09, 6 February 2009, HL Paper 18-I) [88].

[10] Comptroller and Auditor General, 'Progress in tackling benefit fraud' (Department for Work and Pensions, National Audit Office, 23 January, HC 102 Session 2007-2008) p.20.

[11] Comptroller and Auditor General, 'Progress in tackling benefit fraud' (Department for Work and Pensions, National Audit Office, 23 January, HC 102 Session 2007-2008) p.20 (Figure 12).

[12] Comptroller and Auditor General, 'Progress in tackling benefit fraud' (Department for Work and Pensions, National Audit Office, 23 January, HC 102 Session 2007-2008) p.22 (Figure 14).

[13] Department for Work and Pensions, 'Individual Electoral Registration – Confirmation DWP Data Matching Methodology' < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262931/ERTP_CONFIRMATION_DATA_MATCHING_METHODOLOGY.pdf> accessed 22 January 2016.

[14] Department for Work and Pensions, 'Individual Electoral Registration – Confirmation DWP Data Matching Methodology' < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262931/ERTP_CONFIRMATION_DATA_MATCHING_METHODOLOGY.pdf> accessed 22 January 2016 p.11-12.

[15] Department for Work and Pensions, 'Data Matching User Guidance' <https://www.whatdotheyknow.com/request/181664/response/470958/attach/4/Data%20Matching%20User%20Guidance.pdf> accessed 22 January 2016.

[16] Department for Work and Pensions, 'Fraud and Customer Compliance Guidance' <https://www.whatdotheyknow.com/request/181664/response/470958/attach/5/Fraud%20and%20Customer%20Compliance%20guidance.pdf> accessed 22 January 2016 p.2.

Benefit, Employment Support Allowance, Jobseeker's Allowance, Income Support, Central Payment System, Her Majesty's Revenue & Customs, Disability Living Allowance, England & Wales and Scottish Prisoners, Housing Benefit, Industrial Injuries, New Tax Credits, Pension Credit, Customer Information System, Pensions, and Royal Mail Redirect.[17]

2.3 Justifications for the use of the systems

The justifications for the data matching systems in social welfare are twofold. The first justification is combatting fraud. The Government Fraud Review justifies the data sharing by citing savings of hundreds of millions of pounds in various sectors such as the NHS and the National Fraud Initiative.[18] The second justification is improving public services such as how citizens are able to efficiently perform transactions with government departments.[19] This can lead to a citizen's data being analysed centrally and result in them receiving more financial benefits.[20] The DWP's matching system is said to identify claims that have a high risk of being fraudulent, reduce costs and speed up claims for more people.[21]

It is in the public interest to save government money and cut the deficit. It is also beneficial to have central databases where different departments have access to information more readily to expedite social security applications. Both of these justifications are valid and reasonable for the government to attempt to achieve so long as they remain lawful and proportionate.

2.4 Risks and threats

The House of Lords carried out an inquiry into 'the impact that government surveillance and data collection have upon the privacy of citizens and their relationship with the State.'[22] Witnesses before the House of Lords for the inquiry attested to the issues of privacy and individual freedom with regards to this greater level of data collection and surveillance technology used by the government.

With regards to the SSFA, the Information Protection Commissioner expressed concern that confidentiality, transparency, fairness and data security could be undermined. The Information Commissioner is a public official who serves the UK's national data protection authority as required by the DPD. The SSFA has been described as intrusive because once a benefit has been awarded there is continuing suspicion of fraud where the person is surveilled

[17] Department for Work and Pensions to Christina Cruz (15 January 2014) <https://www.whatdotheyknow.com/request/181664/response/470958/attach/3/FOI%202013%204988%20Response.pdf> accessed 22 January 2016.
[18] Select Committee on the Constitution, 'Surveillance: Citizens and the State' (2nd Report of 2008-09, 6 February 2009, HL Paper 18-I) [87].
[19] Select Committee on the Constitution, 'Surveillance: Citizens and the State' (2nd Report of 2008-09, 6 February 2009, HL Paper 18-I) [89-91].
[20] Select Committee on the Constitution, 'Surveillance: Citizens and the State' (2nd Report of 2008-09, 6 February 2009, HL Paper 18-I) [92].
[21] Comptroller and Auditor General, 'Progress in tackling benefit fraud' (Department for Work and Pensions, National Audit Office, 23 January, HC 102 Session 2007-2008) p.21.
[22] Select Committee on the Constitution, 'Surveillance: Citizens and the State' (2nd Report of 2008-09, 6 February 2009, HL Paper 18-I) p.6.

by matching data.[23] The Joint Committee on Human Rights raised concerns that the SSFA, in Parliament before its enactment, could violate Article 8 and 14 of the ECHR.[24] The Committee felt that the power to collect information (that includes, for example, highly sensitive information on health, income, disabilities, education, and business activities) on people because they are part of a particular socio-economic category, or are family members of a person in that category, means the SSFA is open to abuse and could be used in a discriminatory fashion contrary to Articles 14 and 8 of the ECHR.[25] The Secretary of State responded that Article 8 could be restricted for preventing crime and protecting the economic wellbeing of the UK.[26]

The House of Lords highlights that using data system to find trends, and profiling characteristics of classes of people could lead to benefits/welfare being targeted more effectively but individuals or social groups could be discriminated against based on incorrect or misleading data.[27] The Information Commissioner stated with regards to profiling that the temptation to collect all information about all people has the risk of discrimination, social exclusion, stigmatisation and a society where trust is reduced.[28] An example of this is the unrepresentative number of black men on the national DNA register.[29]

2.5 Interim conclusion

The UK has comprehensive data sharing and matching services in use in government departments. Those services are used in conjunction with the law (*i.e.* the SSFA) in combating fraud, saving money and providing a better service for citizens accessing social welfare. Taking into account the large range of personal data the government may access through services listed above, there are a multitude of risks associated with these systems, which include privacy, the danger of stigmatising citizens making social welfare claims, confidentiality and the potential for profiling specific social groups. However, there is no case law as of yet to examine.

When compared to SyRI, it seems that the UK government uses their data processing systems on a larger scale. This is particularly evident when comparing the financial results: whereas SyRI collected € 20.5 million over the course of five years, the UK claims to save hundreds of millions of pounds on a yearly basis. Moreover, it seems that the UK systems may take a

[23] McKeever G, 'Balancing rights and responsibilities: the case of social security fraud' [2009] J.S.S.L. 16(3) p.151.
[24] McKeever G, 'Balancing rights and responsibilities: the case of social security fraud' [2009] J.S.S.L. 16(3) p.152.
[25] Joint Committee on Human Rights, 'Letter from the Chairman of the Committee to the Secretary of State for Social Security' *(*Third Report of 2000-2001, HC 448, Appendix 7).
[26] McKeever G, 'Balancing rights and responsibilities: the case of social security fraud' [2009] J.S.S.L. 16(3) p.152.
[27] Select Committee on the Constitution, 'Surveillance: Citizens and the State' (2nd Report of 2008-09, 6 February 2009, HL Paper 18-I) [34].
[28] Select Committee on the Constitution, 'Surveillance: Citizens and the State' (2nd Report of 2008-09, 6 February 2009, HL Paper 18-I) [112].
[29] Select Committee on the Constitution, 'Surveillance: Citizens and the State' (2nd Report of 2008-09, 6 February 2009, HL Paper 18-I) [113].

more intrusive approach. While intervention teams may use SyRI to support specific small-scale projects, the UK systems can draw on more types of data to detect fraud. Although the data processing systems in the UK differ from SyRI, the same risks apply.

3. Germany

This section contains identified legal issues with regard to data sharing and profiling rising within the jurisdiction of Germany. Although Germany does not have a system similar to SyRI, an analysis of the data protection framework may illustrate some relevant issues.

3.1 Legal framework

The German Federal Data Protection Act[30] (FDPA) implemented the DPD into German law. This law was subject to several major amendments in July 2009 by the Federal Data Protection Act Amendment Law,[31] the majority of which entered into force on 1 September 2009. Although Germany appears not to have a system resembling SyRI, there are several other legislative initiatives that are governed by principles of data protection and data processing.

The German legislator is working on a reform of employee data protection law. This potential new law is expected to clarify the current regime, amongst others on how to treat data of applicants who were not hired. It is also expected to regulate both general and specific aspects of employee data protection, by for instance under specified circumstances allowing medical check-ups as part of application procedures. The German government has furthermore worked on a new act extending the German consumer protection bodies' rights to issue cease and desist letters and to start legal proceedings in case of certain data protection breaches.

Another interesting legal development, in anticipation of the European Network Information Security Directive, is the German Parliament's adoption of the IT Security Act[32] in June 2015 under which so-called critical infrastructures (in particular in the banking, insurance, energy, health, telecoms and transport sectors) must implement and audit state-of-the-art technical and organisational measures regarding their IT. This will likely result in increased data protection for data subjects.

3.2 Overview applicable data sharing or profiling systems

No systems comparable to SyRI have been found in Germany within the scope of this research. This makes any discussion of justifications used for such a potential system unnecessary.

3.3 Risks and threats

There are many security requirements in order to protect personal data in Germany. Public and private bodies which process personal data, either on their own behalf or on behalf of other data controllers, are obliged to take the technical and organisational measures required in the provisions of the FDPA. The minimum requirements the data controller and the data processor must adhere to relate mainly to:

[30] German: 'Bundesdatenschutzgesetz'.
[31] German: 'Novelle des Bundesdatenschutzgesetzes'.
[32] German: 'IT-Sicherheitsgesetz'.

i. access control, related to which persons and entities have access to the date;[33]
ii. processing control, related to the means how and reasons for data processing;[34]
iii. input control, related to the requirements for data to be gathered;[35]
iv. availability control, related to the retention of data;[36] and
v. the separation of data.[37]

There are also specific rules that govern processing by third-party agents. In the event that a data processor is handling personal data on behalf of a data controller, the data processor and the data controller need to conclude a written agreement about the commissioned processing of data. This agreement must include a specific set of minimum requirements containing the standard processor obligations, and some additional requirements such as a description of the object and duration of the processing and an obligation on the data processor to notify the data controller of any security breaches. Where data processors are commissioned to handle data, the responsibility for compliance with the provisions of the FDPA is borne by the data controller. Therefore, the data controller must ensure that the data is processed strictly in accordance with its instructions.

Furthermore, private entities must notify the competent regulatory authority and the persons affected if their data has been unlawfully disclosed to third parties (whether by illegitimate transfer, data leakage or hacker attack) if there is a danger of serious prejudice to the interests of the person affected (for example, the loss of credit card or patient data). If it is too difficult to directly notify all persons affected, a notice must be published in two daily newspapers.

Within the framework of the FDPA, profiling also poses several risks and threats. The NGO Digitalcourage has, amongst others, expressed concerns about the risks involved with profiling.[38] Digitalcourage identifies as a risk that the requirements for the use of profiling are too broad. Authorities or data controllers can use profiling in too many situations, whereas there should actually be a very narrow, specifically defined basis for the use of profiling. The following key issues regarding profiling should be taken into account:

[33] § 5 Federal Data Protection Act (protection of personal data); § 6 Federal Data Protection Act (rights of the data subject); § 15 Federal Data Protection Act (transmission of data to public institutions); § 16 Federal Data Protection Act (transmission of data to non-public institutions).
[34] § 4 Federal Data Protection Act (lawfulness of data gathering, data processing and data use); § 11 Federal Data Protection Act (Gathering, processing or use of personal data on assignment); § 14 Federal Data Protection Act (retention, change and use of data); § 19, 19a, 20 and 21 Federal Data Protection Act (rights of the data subject when data is processed by public institutions); § 33, 34 and 35 Federal Data Protection Act (rights of the data subject when data is processed by non-public institutions).
[35] § 4 Federal Data Protection Act (lawfulness of data gathering, data processing and data use); § 11 Federal Data Protection Act (Gathering, processing or use of personal data on assignment); § 14 Federal Data Protection Act (retention, change and use of data); § 19, 19a, 20 and 21 Federal Data Protection Act (rights of the data subject when data is processed by public institutions); § 33, 34 and 35 Federal Data Protection Act (rights of the data subject when data is processed by non-public institutions).
[36] § 14 Federal Data Protection Act (retention, change and use of data).
[37] § 9 + Annex Federal Data Protection Act (technical measures).
[38] Digitalcourage (2015), *Stellungnahme von Digitalcourage e.V. zur schriftlichen Anhörung zum Entwurf einer Regelung zum Profiling (Art. 20 und Art. 20a)*, Berlin, 5 January 2015

i. Individuals should have an adequate remedy available, not only when the collected data and the results of profiling are put to use, but also against the actual construction of the profile itself;
ii. Individuals should be notified when they are subjected to profiling;
iii. Individuals should have rights concerning the information that is created, they should be able to modify wrongs;
iv. There are several suspicious categories of data which may never be used for any profiling purposes; and
v. Pseudonymisation cannot be regarded as a panacea to the unlimited use of data.[39]

The risks associated with profiling are also related to the legal-technological infrastructure as a whole. To cope with the risks of profiling, a legal-technological infrastructure has to be created that provides society with the legal-technological means to:

i. minimise the leaking of data;
ii. to anticipate which profiles may affect society;
iii. to contest the inherent knowledge claims they entail; and
iv. to challenge their application if necessary.[40]

3.4 Interim conclusion

The German legal framework on personal data processing and data protection offers comprehensive protection to data subjects and provides extensive rules with regard to any form of automatic data processing, including profiling. There is however no system in place which resembles SyRI. As such, a comparison is impossible except for a comparison of the general applicable law. The general applicable law is to a large extent harmonised due to influence of the CoE and the EU legal requirements, but the principles applied in Germany may nonetheless provide an illustration for the assessment of SyRI.

[39] Digitalcourage (2015), *Stellungnahme von Digitalcourage e.V. zur schriftlichen Anhörung zum Entwurf einer Regelung zum Profiling (Art. 20 und Art. 20a)*, Berlin, 5 January 2015
[40] M. Hildebrandt (2006), 'Profiling: From Data to Knowledge', *Datenschutz und Datensicherheit* 30 (2006) 9, p. 552

4. United States

The following section contains an overview of data sharing and profiling systems in the US. The section addresses the legal framework, shows several data processing systems and identifies the risks and threats related to those systems.

4.1 Legal framework

The US protects personal data with more than twenty sector-specific national privacy and data security laws. Additionally, the different states have hundreds of such protection laws.[41] The laws are too diverse to summarise in this report, so this Section only addresses some general and relevant aspects. Firstly, there is no official national data protection authority in the US.[42] Secondly, no legal requirement exists to register databases.[43] Thirdly, US privacy laws generally require that a data controller gives a pre-collection notice before collecting personal data.[44] Fourthly, restrictions apply to the geographic transfer of information.[45] Finally, federal law does not regulate the use of cookies, web beacons and other tracking mechanisms.[46]

The Fourth Amendment of the US Constitution and the Privacy Act of 1974 primarily regulate the conduct of law enforcement agencies with regard to data processing. The Fourth Amendment prohibits 'unreasonable searches and seizures' by the government and thus also applies to data. In this regard the Fourth Amendment offers limited protection since the 'third-party records doctrine' limits the privacy of individuals for personal data that the individual turned over to third parties voluntarily.[47] The Privacy Act of 1974 also offers limited protection: the absence of a comprehensive data protection model for private sources of

[41] DLA Piper, 'Data protection laws of the world', available at <https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=all> last accessed on 17 March 2016, p.414.
[42] DLA Piper, 'Data protection laws of the world', available at <https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=all> last accessed on 17 March 2016, p.414.
[43] DLA Piper, 'Data protection laws of the world', available at <https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=all> last accessed on 17 March 2016, p.415.
[44] DLA Piper, 'Data protection laws of the world', available at <https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=all> last accessed on 17 March 2016, p.415.
[45] DLA Piper, 'Data protection laws of the world', available at <https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=all> last accessed on 17 March 2016, p.415.
[46] DLA Piper, 'Data protection laws of the world', available at <https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=all> last accessed on 17 March 2016, p.417.
[47] Bignami F, 'The US legal system on data protection in the field of law enforcement: Safeguards, rights and remedies for EU citizens' (European Parliament, Directorate General for Internal Policies, Committee on Civil Liberties, Justice and Home Affairs, 2015) p.10.

personal data results in the availability of large amounts of personal data to anyone interested, and thus also to law enforcement agencies.[48]

4.2 Overview applicable data sharing or profiling systems

The US government and law enforcement agencies have numerous automated data processing systems to prevent and combat crime. Many of those systems focus on general security risks, whilst some focus specifically on fraud detection and prevention. In addition, there is a difference between systems that operate nationwide and systems that are only used in a specific State. The following Section shortly outlines four automated processing systems that focus on general security risks, one system that focuses on the detection and prevention of Medicaid, which is applied nationwide and xxx systems that only specific States use.

The US Custom and Border Protection (CBP) use the Automated Targeting System (ATS) to perform background checks and assign terrorist ratings on all US citizens.[49] This happens by performing a risk assessment of every passenger crossing US borders to determine if he or she poses a risk to border security, is a terrorist or suspected terrorist, or otherwise engages in activity violating US law.[50] The CBP also uses the Analytical Framework for Intelligence (AFI) system to collect and develop information concerning persons, cargo and events to better informs the CBP why an individual or cargo may pose a security risk. US Immigration and Customs Enforcement (ICE) use the FALCON environment. Two systems in this environment focus specifically on 'profiling' and 'data sharing': the FALCON Search and Analysis System (FALCON-SA) and the FALCON Data Analysis & Research for Trade Transparency System (FALCON-DARTTS). Both systems create indexes to enable the detection of financial and other anomalies that may form the basis for further investigation.[51] The Federal Bureau of Investigation (FBI) uses the Data Warehouse System to more robustly exchange and compare data between the FBI and numerous other law enforcement agencies.[52] The FBI uses the results coming from such a comparison as leads for investigations.

[48] Bignami F, 'The US legal system on data protection in the field of law enforcement: Safeguards, rights and remedies for EU citizens' (European Parliament, Directorate General for Internal Policies, Committee on Civil Liberties, Justice and Home Affairs, 2015) p.5.

[49] Department of Homeland Security, 'Comments of 30 Organizations and 16 Experts in Privacy and Technology' (Docket No. DH6-2006-0060) p.2; Privacy Office Department of Homeland Security, 'Comments of the Identity Project and John Gilmore' (DHS-2006-0060, 4 December 2006) p.3.

[50] Thompson B, 'Comments of Rep Bennie G. Thompson (D-MS) on Department of Homeland Security Privacy Office Privacy Act System of Records Notice for the US Customs and Border Protection Automated Targeting System' (Docket No. DHS-2006-0060, 2 November 2006) p. 3; Department of Homeland Security, 'Privacy Impact Assessment for the Automated Targeting System' (DHS/CBP/PIA-006, 1 June 2012) p.2.

[51] Department of Homeland Security, 'Privacy Impact Assessment for the FALCON Data Analysis & Research for Trade & Transparency System' (DHS/ICE/PIA-038, 16 January 2014) p.2-3.

[52] Federal Bureau of Investigation, 'Notice of a new system of records: the FBI Data Warehouse System' (Federal Register, Vol. 77:132, 10 July 2012) p.40631.

The Centers for Medicare and Medicaid Services (CMS) use the Medicare-Medicaid Data Match Program to specifically detect and prevent Medicaid fraud and abuse.[53] Medicaid fraud entails that a person knowingly misrepresents the truth to obtain unauthorized benefit, whilst abuse includes any practice that is inconsistent with acceptable fiscal, business or medical practices that unnecessarily increase costs.[54] In 2015, the CMS revealed that the Medicaid improper payment rate jumped from $14.4 billion in 2013 to $29.12 billion in 2015,[55] which shows that Medicaid fraud is a big problem. The CMS apply the Medicare-Medicaid Data Match Program nationwide and receive huge amounts of funding for the application of the system.[56] Over a period of 10 years funding increased to $480 million.[57] The system applies an algorithm to detect payment anomalies and searches for abnormalities such as billing patterns identified with respect to service, time, or patient that raise suspicion or otherwise seem implausible. By sharing and comparing billings from both centres, the algorithm detects patterns of fraud that were previously undetectable for individual programs.[58] In addition, application of the system nationwide ensures that analyses can go deeper to detect anomalies, in comparison to a more superficial analysis at State level.[59]

Only a small number States use data-mining to combat fraud at the State level. These States are: California, Indiana, Louisiana, Michigan, Missouri and Oklahoma.[60] Tennessee, Arkansas, Colorado, Massachusetts, Ohio, South Dakota, Texas and West Virginia have all indicated that the need has not arisen to invest more resources to more effectively detect Medicaid fraud, whilst Hawaii, New Jersey and Rhode Island are evaluating how data-mining could benefit them.[61]

---

[53] Giannangelo K, 'Mining Medicare and Medicaid Data to Detect Fraud' Journal of AHIMA 78(7) (July 2007) 66-67, available at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_034462.hcsp?dDocName=bok1_034462.

[54] National Conference of State legislatures, 'Medicaid fraud and abuse'(Last updated April 2013), availabla at http://www.ncsl.org/research/health/medicaid-fraud-and-abuse.aspx.

[55] Dickson V, 'HHS wants more states to data-mine for Medicaid fraud' (16 December 2015) available at http://www.modernhealthcare.com/article/20151216/NEWS/151219895.

[56] Centres for Medicare and Medicaid Services, 'The Deficit Reduction Act: Important Facts for State Government Officials' p. 5.

[57] Giannangelo K, 'Mining Medicare and Medicaid Data to Detect Fraud' Journal of AHIMA 78(7) (July 2007) 66-67, available at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_034462.hcsp?dDocName=bok1_034462.

[58] Giannangelo K, 'Mining Medicare and Medicaid Data to Detect Fraud' Journal of AHIMA 78(7) (July 2007) 66-67, available at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_034462.hcsp?dDocName=bok1_034462.

[59] Giannangelo K, 'Mining Medicare and Medicaid Data to Detect Fraud' Journal of AHIMA 78(7) (July 2007) 66-67, available at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_034462.hcsp?dDocName=bok1_034462.

[60] Dickson V, 'HHS wants more states to data-mine for Medicaid fraud' (16 December 2015) available at http://www.modernhealthcare.com/article/20151216/NEWS/151219895.

[61] Dickson V, 'HHS wants more states to data-mine for Medicaid fraud' (16 December 2015) available at http://www.modernhealthcare.com/article/20151216/NEWS/151219895.

4.3 Justifications for the use of the systems

The US government often justifies the use of data processing systems by referring to some general advantages relating to the use of those systems, which would not come into play if the government would not use the programmes. Investigators have for example concluded that the government could have prevented terrorist attacks if law enforcement agencies would have had the ability to connect dots in information they already had access to.[62] Automated processing systems, which analyse enormous amounts of data, do connect these dots. This therefore justifies their use.[63] This justification is based on the argument that the use of technology can lead to the more effective detection, prevention and combating of crime.[64]

The US Government justifies the use of the five systems on similar grounds. The use of the ATS has the purpose of effectively ensuring aviation security and, effectively ensuring that people with harmful intentions regarding the US are not admitted into the country.[65] The same applies for the AFI system since it 'improves the efficiency and effectiveness of CBP's research and analysis process by providing a platform for the research, collaboration, approval, and publication of finished intelligence products'.[66] FALCON-SA and FALCON DARTTS in turn assist human research, evaluation, decision-making and analysis in order to avoid error-making and analytic uncertainty.[67] The FBI Data Warehouse System enables more comprehensive analysis of information through the centralized data warehouses.[68] More effective and comprehensive processing of data to provide more national security is thus an essential justification for the use of automated data processing systems.

[62] Dahl E, 'Preventing Terrorist Attacks: Challenging the Conventional Wisdom' (Belfer Center, Harvard University John F. Kennedy School of Government, Policy Memo, 5 May 2008) p.1; Atkinson R, Castro D, 'Digital Quality of Life: Understanding the Personal & Social Benefits of the Information Technology Revolution' (The Information Technology and Innovation Foundation, October 2008) p.117.

[63] Atkinson R, Castro D, 'Digital Quality of Life: Understanding the Personal & Social Benefits of the Information Technology Revolution' (The Information Technology and Innovation Foundation, October 2008) p.117-118.

[64] Atkinson R, Castro D, 'Digital Quality of Life: Understanding the Personal & Social Benefits of the Information Technology Revolution' (The Information Technology and Innovation Foundation, October 2008) p.118.

[65] Electronic Privacy Information Centre, 'Comments of the Electronic Privacy Information Centre to the US Customs and Border Protections of the Department of Homeland Security' (DHS Docket Nos. 2012-0019 and 2012-0020) 21 June 2012 p.2; Department of Homeland Security, 'Privacy Impact Assessment for the Automated Targeting System' (DHS/CBP/PIA-006, 1 June 2012) p. 19.

[66] Department of Homeland Security, 'Privacy Impact Assessment for the Analytical Framework for Intelligence (AFI)' (1 June 2012) p. 2, 7.

[67] Department of Homeland Security, 'Privacy Impact Assessment for the FALCON Search & Analysis System' (DHS/ICE/PIA-032(a), 16 January 2014) p. 2; Department of Homeland Security, 'Privacy Impact Assessment for the FALCON Data Analysis & Research for Trade & Transparency System' (DHS/ICE/PIA-038, 16 January 2014) p 3.

[68] Federal Bureau of Investigation, 'Notice of a new system of records: the FBI Data Warehouse System' (Federal Register, Vol. 77:132, 10 July 2012) p.40632.

4.4 Merits of the justifications

Whether the use of automated data processing systems really leads to more effective crime detection, prevention and combatting is hard to evaluate. The systems undoubtedly can more easily make connections and discover correlations that a human mind cannot make or discover, but it is unclear whether these connections and correlations justify the conclusion that there a security risk exists in every situation. Another relevant question is at what cost the extra effectiveness should and may come. This question is linked to the risks and threats related to the use of automated data processing systems.

4.5 Risks and threats

The use of the systems displayed above creates several risks and threats. The following Section firstly identifies risks related to protection by the law, secondly, risks related to data and processing quality, thirdly, risks related to transparency and fourthly, risks related to oversight and accountability.

The Privacy Act 1974 regulates the conduct of law enforcement agencies with regard to data processing. Several provisions of the Privacy Act 1974 do however not apply to some of the systems. The Privacy Act provides important protection from government conduct, which does not apply to the US government using the ATS and the Data Warehouse System.[69] The inapplicability of such provisions enhances the chance of violations of the right to private and family life and other data protection principles.

Several risks exist related to the quality of the data and the processing: there is a great lack of control over which data agencies share information to other agencies or even to private entities.[70] Virtually unlimited possibilities exist for agencies to disclose data to other agencies.[71] In addition the agencies can use information regarding racial or ethnic origin for assessments, which can lead to discrimination.[72] If information in the system is flawed in

[69] Federal Bureau of Investigation, 'Notice of a new system of records: the FBI Data Warehouse System' (Federal Register, Vol. 77:132, 10 July 2012) p.40633.

[70] Thompson B, 'Comments of Rep Bennie G. Thompson (D-MS) on Department of Homeland Security Privacy Office Privacy Act System of Records Notice for the US Customs and Border Protection Automated Targeting System' (Docket No. DHS-2006-0060, 2 November 2006) p. 4; Electronic Privacy Information Centre, 'Comments of the Electronic Privacy Information Centre to the US Customs and Border Protections of the Department of Homeland Security' (DHS Docket Nos. 2012-0019 and 2012-0020, 21 June 2012) p.9.

[71] Department of Homeland Security, 'Comments of 30 Organizations and 16 Experts in Privacy and Technology' (Docket No. DH6-2006-0060) p.14-15; Electronic Privacy Information Centre, 'Comments of the Electronic Privacy Information Centre to the US Customs and Border Protections of the Department of Homeland Security' (DHS Docket Nos. 2012-0019 and 2012-0020, 21 June 2012) p.9; Department of Homeland Security, 'Privacy Impact Assessment for the FALCON Search & Analysis System' (DHS/ICE/PIA-032(a), 16 January 2014) p. 20; Department of Homeland Security, 'Privacy Impact Assessment for the FALCON Data Analysis & Research for Trade & Transparency System' (DHS/ICE/PIA-038, 16 January 2014) p.23.

[72] Electronic Privacy Information Centre, 'Comments of the Electronic Privacy Information Center to Department of Homeland Security' (Docket Nos. DHS-2007-0042 and DHS-2007-0043, 5 September 2007) p.14-15, p. 10; Electronic Privacy Information Centre, 'Comments of the Electronic Privacy Information Centre to the US Customs and Border Protections of the Department of Homeland Security' (DHS Docket Nos. 2012-0019 and 2012-0020, 21 June 2012) p.4, 8.

general, this may lead to mismatches by the system.[73] In such a situation the information does not indicate illegal activity, although this risk also exists with the use of correct data.[74] Moreover, agencies may use data for other purposes than for which it was collected in the first place.[75] Finally, taking the purpose of the system and the reason of collection into account, agencies may store the data for a longer period than necessary and appropriate.[76]

Agencies are not transparent with regard to the use of the numerous data processing systems. They do not provide information on how the systems operate and they do not disclose information regarding the different functions of the systems.[77] This again prevents discovery of violations of individuals' rights through misuse of the systems. In addition, the agencies do not inform the public that the systems collect, share and analyse their personal data.[78] Those individuals do not have the opportunity to consent, opt-out, or decline to have their information included into the systems.[79]

An independent institution does not monitor and evaluate the systems.[80] This again has an effect on the detection of misuse of the systems. In addition, individuals cannot hold the responsible agencies to account since often no enforceable right for individuals to access or correct information exists.[81]

---

[73] Electronic Privacy Information Centre, 'Comments of the Electronic Privacy Information Center to Department of Homeland Security' (Docket Nos. DHS-2007-0042 and DHS-2007-0043, 5 September 2007) p.14-15; Department of Homeland Security, 'Privacy Impact Assessment for the FALCON Search & Analysis System' (DHS/ICE/PIA-032(a), 16 January 2014) p.12; Department of Homeland Security, 'Privacy Impact Assessment for the FALCON Data Analysis & Research for Trade & Transparency System' (DHS/ICE/PIA-038, 16 January 2014) p.13.

[74] Department of Homeland Security, 'Privacy Impact Assessment for the Analytical Framework for Intelligence (AFI)' (1 June 2012) p.17.

[75] Department of Homeland Security, 'Privacy Impact Assessment for the Analytical Framework for Intelligence (AFI)' (1 June 2012) p.8, 13, 16, 20; Department of Homeland Security, 'Privacy Impact Assessment for the FALCON Search & Analysis System' (DHS/ICE/PIA-032(a), 16 January 2014) p.12, 15; Department of Homeland Security, 'Privacy Impact Assessment for the FALCON Data Analysis & Research for Trade & Transparency System' (DHS/ICE/PIA-038, 16 January 2014) p.14, 19.

[76] Department of Homeland Security, 'Privacy Impact Assessment for the FALCON Search & Analysis System' (DHS/ICE/PIA-032(a), 16 January 2014) p.18; Department of Homeland Security, 'Privacy Impact Assessment for the FALCON Data Analysis & Research for Trade & Transparency System' (DHS/ICE/PIA-038, 16 January 2014) p.22.

[77] Department of Homeland Security, 'Comments of 30 Organizations and 16 Experts in Privacy and Technology' (Docket No. DH6-2006-0060) p.4.

[78] Department of Homeland Security, 'Privacy Impact Assessment for the Analytical Framework for Intelligence (AFI)' (1 June 2012) p.17; Department of Homeland Security, 'Privacy Impact Assessment for the FALCON Search & Analysis System' (DHS/ICE/PIA-032(a), 16 January 2014) p.17; Department of Homeland Security, 'Privacy Impact Assessment for the FALCON Data Analysis & Research for Trade & Transparency System' (DHS/ICE/PIA-038, 16 January 2014) p.20.

[79] Department of Homeland Security, 'Privacy Impact Assessment for the FALCON Search & Analysis System' (DHS/ICE/PIA-032(a), 16 January 2014) p.17.

[80] Department of Homeland Security, 'Comments of 30 Organizations and 16 Experts in Privacy and Technology' (Docket No. DH6-2006-0060) p.2.

[81] Department of Homeland Security, 'Comments of 30 Organizations and 16 Experts in Privacy and Technology' (Docket No. DH6-2006-0060) p.3, 6, 8.

4.6 Interim conclusion

The US government uses several data sharing and profiling systems. This section identified multiple risks related to the use of these systems. These risks are: limited protection by the law, use of incorrect or biased data and other risks related to the quality of the data, a lack of transparency, and a lack of oversight and accountability.

The five data processing systems in Section 4.2 all process data to detect, prevent and combat different forms of crime. The first four systems however do not focus on the detection of fraud. Especially the Medicare-Medicaid Data Match Program resembles SyRI since it processes personal data, by searching for anomalies through the application of an algorithm, to detect and prevent Medicaid fraud and abuse. The big amount of funding that the CMS receive seems to indicate that the US government uses the system more often than the Dutch government uses SyRI. If it is the case that the US government uses the system on a much larger scale and more often, this will likely lead to more mistakes and violations of data subjects' rights, creating more risks. Similar risks identified in section 4.5 also apply to SyRI. Not only is there a great lack of transparency with regard to the use of SyRI and the compliance of data controllers with data protection principles, there is also a lack of oversight for the monitoring of such compliance, even though the protection by the law does seem to be adequate with regard to SyRI. Moreover, the different levels of analysis in SyRI do seem to ensure that incorrect or incomplete data does not form a basis for a risk notification.

5. Conclusion

This memorandum firstly illustrated the status of the legal frameworks regarding data processing and data protection in three jurisdictions: the UK, Germany and the US. The research has focused on identifying specific data sharing systems resembling SyRI as well. The UK has a similar legal framework for data sharing in relation to social welfare fraud in the form of the Social Security Fraud Act 2001 and the Welfare Reform Act 2012. The US does not have a system as similar as the UK has, but the most resembling system is the Medicare-Medicaid Data Match Program which shares and processes data with the purpose of preventing healthcare fraud. Within the parameters of the research, no system in Germany was found which shares data between governmental institutions with the purpose of the prevention of fraud. The legal framework regarding data protection is however quite extensive. Moreover, no case law was found related to data processing to combat fraud. An explanation for this is that intervention teams will use risk notifications as a starting point for further investigation. The initial notification will therefore not be used as evidence and will thus seldom be scrutinised.

Systems with similar objectives as SyRI, namely the prevention of social welfare fraud, were analysed with regard to the UK and the US. The jurisdiction's national justifications for use of the systems were always the combatting and prevention of fraud and meeting the public demand to prevent crime and misuse of public goods. This is identical to the justifications for the use of SyRI in the Netherlands.

Lastly, the risks and threats were examined for each jurisdiction's respective systems. This provided conclusions on the merits and shortfalls of systems such as SyRI and systems that share different types of data but still have similar risks to that of SyRI. These risks include:

- violations of the right to privacy;
- the danger of stigmatising citizens making social welfare claims and the related potential of profiling specific social groups as such possibly leading to discrimination or unequal treatment;
- infringements of confidentiality of personal data;
- limited protection of data subjects by the law, use of incorrect or biased data and other risks related to the quality of the data;
- a lack of transparency of the data processing measures; and
- a lack of oversight and accountability
- a lack of redress.

Many of these risks also apply to the use of SyRI. In particular, the lack of transparency is a serious problem within SyRI. Although it seems that data controllers comply with most of the data protection principles, the lack of transparency makes it hard to determine whether this is really the case. An apparent lack of internal oversight makes this all the more problematic. The lack of transparency and internal and external oversight is a risk that thus appears in processing systems worldwide.