Oxford Pro Bono Publico
http://www.law.ox.ac.uk/opbp

BIOMETRIC IDENTIFICATION AND PRIVACY

Comparative research prepared for the Centre for Law and Policy Research, India

February 2013

CONTRIBUTORS

Faculty:

Dr David Erdos
Katzenbach Research Fellow &
Leverhulme Trust Early Career Fellow

Research coordinators:

Chintan Chandrachud
OPBP Treasurer
MPhil Candidate

Chris McConnachie
OPBP Chairperson
DPhil Candidate

Tamas Szigeti
OPBP Events and Liaison Officer
MPhil Candidate

Researchers:

Lauren Dancer
BCL Candidate

Julian Ensbey
BCL Candidate

Natasha Holcroft-Emmess
BCL Candidate

Anjoli Maheswaran Foster
BCL Candidate

Ram Mashru
MSc in Contemporary India Candidate

Angela Pavao
MSt in Criminology Candidate

Sarah Tulip
BCL Candidate

Mark Zarwi
BCL Candidate

The research coordinators would like to thank:

- **Professor Timothy Endicott**, Dean of the Oxford Law Faculty, for his support of this project;
- The Members of the Oxford Pro Bono Publico Executive Committee, **Professor Sandra Fredman**, **Dr Tarunabh Khaitan, Mr Miles Jackson, Ingrid Cloete, Emma Webber,** and **Richmond Glasgow**, for their support and assistance with the project.

Indemnity

Oxford Pro Bono Publico (OPBP) is a programme run by the Law Faculty of the University of Oxford, an exempt charity (and a public authority for the purpose of the Freedom of Information Act). The programme does not itself provide legal advice, represent clients or litigate in courts or tribunals. The University accepts no responsibility or liability for the work which its members carry out in this context. The onus is on those in receipt of the programme's assistance or submissions to establish the accuracy and relevance of whatever they receive from the programme; and they will indemnify the University against all losses, costs, claims, demands and liabilities which may arise out of or in consequence of the work done by the University and its members.

Intellectual property

TABLE OF CONTENTS

PART A

SUMMARY OF RESEARCH

INTRODUCTION

1. This report has been prepared to assist the Centre for Law and Policy Research in drafting a petition to the Supreme Court of India, challenging the constitutional validity of the Unique Identification Number (UID) scheme, otherwise known as the 'Aadhaar' scheme.

2. The UID scheme aims to issue all 1.2 billion Indian residents with a universal identification number, linked with biometric and demographic data that will be stored on a centralised database. Three types of biometric data will be collected: facial photographs, finger prints and iris scans.[1] If completed, this will be world's largest biometric database. However, India currently lacks comprehensive data privacy protection laws and the draft National Identification Authority of India Bill 2010 contains limited safeguards.[2]

3. OPBP has been requested to prepare research on two questions:
    a. Have biometric identification schemes in other countries been challenged on privacy grounds?
    b. In jurisdictions that collect biometric data, what measures are in place to protect citizens' right to privacy?

4. Our research covers eight jurisdictions, selected because they use biometric identification schemes and based on the expertise of our researchers. These are the United States of America (US), Israel, Australia, the Council of Europe, the European Union (EU), the United Kingdom (UK), France, and Germany.

5. This report consists of two parts. This part, Part A, provides a summary of our research, drawing out key points that are relevant to the petition challenging the UID scheme. Part B provides information on the specific jurisdictions, dividing the discussion of each jurisdiction into three sections: an overview of the jurisdiction,

[1] For the purposes of this report, biometric data is defined as data relating to an individual's physiological and behavioural characteristics, allowing for individual identification or verification. See EU Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, 'Working Paper 80: Working document on biometrics' (2003) 12168/02/EN, 2.

[2] See Graham Greenleaf, 'India's national ID system: Danger grows in privacy vacuum' (2010) 26 Computer Law & Security Review 479, 480 and 487.

the relevant legal framework, and the relevant case law on biometric identification schemes. Where there is no case law, we have considered the political debates over these schemes. We hope that Part B will be useful should the Centre for Law and Policy Research wish to explore the issues discussed in this summary in greater detail.

6. This summary covers four topics:
    a. Background;
    b. Biometric information and the right to privacy;
    c. The justification of interferences with privacy rights;
    d. Safeguards for the protection of biometric data.

BACKGROUND

7. In the US, Israel, France, and Germany, the right to privacy is constitutionally and legislatively protected. In these jurisdictions, either the written constitutions have expressly enumerated the right to privacy or one of their provisions has been interpreted as including this right. The European Convention on Human Rights (applicable in the Council of Europe Member States) and the European Charter on Fundamental Rights and Freedoms (applicable in the EU) expressly contain a right to privacy. In Australia and the UK,[3] although the right to privacy is not constitutionally protected, it is protected by primary legislation.

8. All of the jurisdictions in our study have data protection laws which apply to personal data. In the European context, 'personal data' is defined as 'any information relating to an identified or identifiable individual'.[4] Biometric data is considered to be a class of personal data and is therefore subject to protection.[5] A similar approach has been adopted in the US,[6] Israel,[7] and Australia.[8]

---

[3] The UK does not have a written constitution, in the sense of a codified document.
[4] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data European Treaty Series No 108; adopted 28 Jan 1981 (Council of Europe Convention), art 2(a) (Data Protection Convention); EU Council 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 [1995] OJ L281/31, art 2(1) (EU Directive).
[5] See EU Working Party, 'Working Paper' (n 1) section 3.1. See further *S and Marper v UK* (2009) 48 EHRR 50 discussed at para 10 below.
[5] Council Directive 95/46/EC (n 4) art 8(1).
[6] See United States, para 35 below.
[7] See Israel, para 56 below.
[8] See Australia, para 66 below.

9. Biometric identification schemes are in operation in all of the jurisdictions considered in this study. The purposes of these schemes are diverse and include the prevention of crime,[9] immigration control,[10] identity protection[11] and the maintenance of security standards for passports.[12]

BIOMETRIC INFORMATION AND THE RIGHT TO PRIVACY

10. In the European context, the collection of personal data in databases by the state, including the collection of biometric data, is generally considered to be an interference with the right to privacy, requiring justification.[13]

11. In *S and Marper v United Kingdom*[14] the European Court of Human Rights (ECtHR) held that:

> [T]he mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data.[15]

The applicants were arrested and charged with criminal offences in the UK. One of the applicants was acquitted and the case against the other was discontinued. Deciding on whether it was permissible for the UK police to retain fingerprints, cellular samples and DNA samples collected from the applicants, the Grand Chamber of the ECtHR observed that these data fell within the realm of 'personal data' and the retention and storage of these data was an interference with the applicants' Article 8(1) right to a private life under the European Convention on Human Rights (ECHR).[16] The Court ultimately found that this interference was disproportionate.[17]

---

[9] See discussions on the US (paras 27-30 below) and France (paras 118-120 below).
[10] See US, para 28.
[11] See Israel (para 52 below), France (para 115 below), UK (para 106 below).
[12] See in particular EU, para 93-94.
[13] The European Court of Human Rights appeared to affirm this position in *Marper* (see n 14 below), but its Art 8 jurisprudence under the European Convention on Human Rights is not yet settled.
[14] *S and Marper v UK* (2009) 48 EHRR 50.
[15] ibid [121].
[16] ibid [121].
[17] ibid [125]. Discussed further below at para 23.

12. The German Federal Constitutional Court adopted a similar approach in the *Census Act Case*.[18] This case involved a challenge to the National Census Act 1983, which placed an obligation on every household to fill in and return a census form for the collection of statistical data. There the Court held that the protection of 'informational self-determination' fell within the ambit of the 'right to the free development of one's personality' under article 2(1) of the German Constitution:

> Individual self-determination, however, presupposes – even under the conditions of modern information processing techniques – that the individual has the freedom to decide whether to perform or omit actions, including the possibility of acting according to this decision. A person who cannot safely tell what information about him regarding certain areas is known to his social environment, and cannot to some extent assess the knowledge of potential partners of communication, can be essentially inhibited in his freedom to make autonomous plans and decisions. … *It follows that the free development of one's personality under the modern conditions of data processing presupposes the protection of the individual against unlimited collection, storage, use and transmission of his personal data.*[19]

13. In a 2012 decision, the French Constitutional Court, the *Conseil Constitutionnel*, affirmed a similar principle in striking down portions of a law authorising the implementation of a national biometric identification scheme and the creation of a national biometric database.[20] The *Conseil* held that biometric data constitute 'personal data' and that the right to respect for private life under the French Constitution requires that:

> [T]he collection, registration, conservation, consultation and communication of personal data must be justified on grounds of general interest and implemented in an adequate manner, proportionate to this objective.[21]

14. The US Supreme Court has also confirmed that the right to privacy under the US Constitution includes 'an individual interest in avoiding disclosure of personal

---

[18] BVerfG 15 December 1983, *BVerfGE* 65, 1, 43 – *Census Act Case ('Volkszählung'),* discussed in S Michalowski and L Woods, *German constitutional law: the protection of civil liberties* (Ashgate 1999) 120-123.
[19] ibid 42-43 (emphasis added).
[20] Décision n° 2012-652 DC du 22 mars 2012 (Official English translation available at <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/pdf/conseil-constitutionnel-105428.pdf> accessed 21 February 2013).
[21] ibid [8].

matters'.[22] However, the US is distinct from the European jurisdictions in that it does not engage in a two-stage balancing exercise. Instead, justificatory considerations are built into the enquiry whether the right to privacy has been violated, with the result that mere collection, storage, or disclosure of personal data are not considered to be automatic violations of this right.[23]

THE JUSTIFICATION OF INTERFERENCES WITH PRIVACY RIGHTS

15. The jurisdictions considered in this report apply different tests in ascertaining whether the restrictions imposed on the right to privacy are justified. Courts in the EU and the Council of Europe apply a three-part test requiring that limitations must: (a) be in accordance with the law; (b) serve a legitimate aim; and (c) be 'necessary in a democratic society'.[24] The last requirement involves a proportionality analysis, requiring the Court to determine whether the limitation is suitable for achieving its aim (suitability), whether there are less restrictive means to achieve this aim (necessity), and whether the extent of the limitation is outweighed by the achievement of the aim (proportionality in the 'narrow sense').[25]

16. In the US, a softer standard of review has been applied in privacy cases, with courts largely focussing on the rationality of legislative restrictions on the right to privacy.[26] However, the degree of deference accorded by courts to the legislature and the executive has often depended upon the nature of the information sought to be collected. In *Whalen v Roe*,[27] a statute that required physicians to report details of patients to whom they had prescribed certain drugs was challenged on privacy grounds. Although the US Supreme Court concluded that the statute did not constitute a violation of the right to privacy, Justice Brennan observed that '[t]he central storage and easy accessibility of computerized data vastly increase[d] the potential for abuse of that information' and that future developments might compel

[22] *Whalen v Roe*, 429 US 589, 97 S Ct 869, 51 L Ed 2d 64, Stevens J at 599. The Supreme Court has held that privacy interests are protected under the 1st, 4th and 14th Amendments of the Constitution. See *Katz v United States*, 389 U.S. 347 (1967), *Griswold v Conneticut,* 381 US 479, 85 S. Ct. 1678 and *Stanley v Georgia*, 394 U.S. 557 (1969).
[23] See US, para 41ff below.
[24] See Council of Europe, paras 73-74; EU, para 87.
[25] See Aharon Barak, *Proportionality: Constitutional Rights and Their Limits* (CUP 2012) chs 9-12.
[26] See *Whalen v Roe* (n 22) 597. See also *Thom v New York Stock Exchange*, 306 F Supp 1002 (1969) 1011; *Iacobucci v City of Newport, Ky*, 785 F 2d 1354 (1986) 1355.
[27] ibid.

'some curb on such technology'.[28] Further, courts have looked upon databases storing 'sensitive information' (as the term is understood in the US) with a more critical eye. In *US v Westinghouse*,[29] the Court of Appeals for the Third Circuit declined a challenge to a subpoena granted to a health and safety inspector mandating an employer to disclose its employees' medical records. The Court held that the constitutional right to privacy had not been breached, since the information contained in the medical records was not 'sensitive'.[30] It laid down a number of factors that should be considered in deciding whether an individual's right to privacy was violated, including 'the type of record…the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated'.[31] The point was put clearly by the Court of Appeals for the Ninth Circuit in *Doe v Attorney General*: 'the more sensitive the information, the stronger the state's interest must be'.[32]

17. The US understanding of 'sensitive information' should be contrasted with the definition of 'sensitive data' in other jurisdictions. In Europe and jurisdictions inspired by the European data protection model, sensitive data is defined as personal data revealing certain protected characteristics, including 'racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life [and]… relating to criminal convictions'.[33] Some, but not necessarily all, types of biometric data may be classified as sensitive information. The EU Working Party on the Protection of Individuals with Regard to the Processing of Personal Data suggests that facial images in particular should be regarded as sensitive data as they have the potential to reveal ethnic or racial origin.[34] Sensitive data is subject to heightened safeguards and may not be automatically processed except in defined circumstances. In Australia, the Privacy

[28] ibid 607.
[29] 638 F 2d 570.
[30] ibid 579.
[31] ibid 578.
[32] 941 F2d 780.
[33] See Data Protection Convention (n 4) art 6; EU Directive (n 4) art 8.
[34] Working Party, 'Working document on biometrics' (n 1) 10. The Working Party is comprised of representatives from data protection authorities in all EU Member States, the European Data Protection Supervisor, and a representative of the EU Commission. See Council Directive 95/46/EC (n 4), art 29.

Act 1998 was recently amended to include all biometric data as 'sensitive information', which must be managed with particular care.[35]

18. Other types of data that have resulted in courts being less deferential include data with personal references (which are not anonymised or statistically prepared)[36] and personal data that have undergone automatic processing.[37]

SAFEGUARDS FOR THE PROTECTION OF BIOMETRIC DATA

a) Legal safeguards

19. Given that the collection, processing and storage of biometric data are generally considered to be interferences with the right to privacy, adequate legal safeguards are required for these interferences to be justified. In General Comment 16 on the article 17 right to privacy in the International Covenant on Civil and Political Rights, the Human Rights Committee emphasised that:

> The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorises or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[38]

Similarly, in *Marper*, the ECtHR stressed that:

> The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private… life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent

---

[35] The amendment was made by the Privacy Amendment (Enhancing Privacy Protection) Act 2012, Schedule 1, s 42.
[36] *Census Act Case* (n 18).
[37] *S and Marper v UK* (n 14) [103].
[38] UNHRC 'General Comment 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art 17)' (1988) [10] <http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/23378a8724595410c12563ed004aeecd?Opendocument> accessed 21 February 2013.

> any such use of personal data as may be inconsistent with the guarantees of this Article. The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned … The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored. The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse … .[39]

b) Common features of safeguards

20. The countries in this study have adopted very similar legal safeguards governing the collection, use and storage of personal data, including biometric data. These safeguards are framed and applied in somewhat different ways, but they share at least nine common features:[40]

a. **Purpose specification**: Data must be collected for specified, explicit and legitimate purposes.
b. **Data quality:** Data collected should be relevant and necessary to accomplish the legitimate purposes for which it is being collected.
c. **Data collection:** Data should be given with the consent or knowledge of the data subjects.
d. **Notice:** Data subjects should be informed about the purposes for which the data are being collected, the authority authorising data collection, whether disclosure is mandatory or voluntary, and the consequences of non-provision, among other matters.
e. **Limitations on use:** The data should only be used for the purposes originally specified, or purposes compatible with those purposes. Restrictions also apply to the transfer of data between state organs and between the state and private organisations or individuals.
f. **Security:** Appropriate security measures should be in place to ensure the security, integrity and confidentiality of personal data.
g. **Access:** Data subjects should have a right to access their personal data held in databases.

[39] *S and Marper v UK* (n 14) [103].
[40] What follows is adapted from Graham Greenleaf's ten 'universal' elements of global privacy law, outlined in Graham Greenleaf, 'The influence of European data privacy standards outside Europe: implications for globalization of Convention 108' (2012) 2 International Data Privacy Law 68, 73.

h. **Correction:** Data subjects should have the right to update and correct this data.

i. **Independent data protection authority:** All jurisdictions in this study also provide for an independent data protection authority to monitor compliance with data privacy safeguards and to investigate and act on complaints.

21. As noted above, European and European-inspired jurisdictions also require heightened safeguards for 'sensitive data', relating to certain protected characteristics.[41]

c) Challenges to biometric identification schemes

22. Our research has identified three recent cases involving challenges to biometric identification schemes: the ECtHR's decision in *S and Marper v United Kingdom*,[42] the petition against Israel's biometric identification scheme in *Nahon v Knesset*,[43] and the French *Conseil Constitutionnel* decision on the national biometric identity card scheme.[44] In these cases, the existence and adequacy of legal safeguards were central to the courts' assessment of whether these interferences with the right to privacy were justified.

i) S and Marper v United Kingdom

23. As introduced above, in *Marper* the applicants argued that the UK police's retention of their fingerprints, cellular samples and DNA profiles after charges against them were dropped was inconsistent with the right to respect for private life enshrined in Article 8 ECHR. In assessing whether this interference was proportionate, the Court placed weight on the fact that the UK was the only Member State of the Council of Europe which permitted indefinite retention of fingerprint and DNA data.[45] It compared the practice of the majority of other Member States, which required such samples to be removed or destroyed either immediately or within a certain time after acquittal or discharge.[46] The blanket and indiscriminate nature of its powers of retention meant that the UK had overstepped its margin of

[41] Above para 17.
[42] Above n 14.
[43] HCJ 1516/12 *Nahon v. Knesset* S.CT 842 (2012) (judgment available in Hebrew) <http://elyon1.court.gov.il/files/12/160/015/c03/12015160.c03.htm> accessed 21 February 2013.
[44] Above n 20.
[45] ibid [110].
[46] ibid [108].

appreciation and failed to strike a fair balance between the competing public and private interests. Accordingly, the retention of the applicants' data was a disproportionate interference with their right to respect for private life and a constituted a violation of Article 8 ECHR.[47]

24. The Grand Chamber's approach in *Marper* therefore indicates that a national system of collection and retention of biometric information must incorporate sufficient safeguards in order adequately to protect the right to respect for private life under the ECHR. It appears that by 'appropriate safeguards', the Court means that the law must include requirements against indefinite storage.[48]

ii) Nahon v Knesset

25. The necessity of collecting biometric data in a centralised database was debated in the Israeli High Court of Justice in *Nahon v Knesset*.[49] The petitioners challenged the Israeli Law for Including Biometric Identifying Means and Data in Documents of Identification and in Databases 2009 and a proposed two-year pilot programme to test biometric identification. The legislation provides for the embedding of biometric data (fingerprints and computerized tags of facial features) in Israeli identification cards and passports, and allows for the creation of a database containing biometric data on all Israeli citizens.[50] The petitioners specifically challenged the creation of a central database of biometric identification, arguing that this was not necessary to achieve the purpose of accurately identifying Israeli citizens.[51] It was argued that it was possible to embed biometric data on smart ID cards and to check identity against these cards, without creating a centralised database. The Court ultimately dismissed the petition as premature, given that the pilot programme had not yet been completed. However, at the hearing the Justices strongly criticised the scheme, demanding that the Interior Ministry rework its planned pilot programme to evaluate whether it is actually *necessary* to store the population's biometric data in a single, centralized database. In the wake of the

[47] ibid [125].
[48] For further discussion of this case see Council of Europe, para 78 below.
[49] Above n 43.
[50] Rawlson King, 'Israeli jurists right to call biometric database "extreme" and "harmful"' *BiometricUpdate.com* (30 July 2012) <www.biometricupdate.com/201207/israeli-jurists-right-to-call-biometric-database-extreme-and-harmful/> accessed 21 February 2013.
[51] The Association for Civil Rights in Israel, 'Introduction from ACRI Petition to the High Court of Justice: Objections to a Governmental Biometric Database' (February 2012) <http://www.acri.org.il/en/wp-content/uploads/2012/02/biometric.pdf> accessed 21 February 2013.

2006 theft and dissemination of Israel's Population Registry, containing data on nine million Israeli citizens, the Justices were particularly concerned that a centralised biometric database would bring greater security risks.[52] Since the hearing, the Interior Ministry has been exploring other options,[53] as well as evaluating safeguards to prevent data leaks and information theft.[54]

iii) Conseil Constitutionnel decision

26. In 2012, the French Constitutional Court, the *Conseil Constitutionnel* (*Conseil*), struck down portions of legislation which introduced a national identity card containing biometric information (face image and fingerprints), and provided for the creation of a national database for this data.[55] The court found that the Act served the legitimate aim of preventing identity fraud. However, the *Conseil* found that the legislation exceeded this legitimate purpose by authorising the police and other law enforcement agencies to access the database for purposes unrelated to the prevention of fraud.[56] Therefore, the *Conseil* found that this was a disproportionate restriction of the right to privacy.[57] It should be noted, however, that the *Conseil* did not take issue with the creation of a population-wide biometric database per se.[58]

[52] See Israeli Ministry of Justice, 'Theft and Online Dissemination of Israel's Population Registry' <http://www.justice.gov.il/MOJEng/ILITA/News/crackedcase.htm> accessed 21 February 2013.
[53] ibid.
[54] For further discussion of this case see Israel, para 58 below.
[55] Above n 20.
[56] ibid [10]: 'that the technical characteristics of this database as defined by the contested provisions enable it to be consulted for purposes that other than the verification of an individual's identity.' (Official English translation)
[57] ibid [3].
[58] For further discussion of this case see France, para 115 below.

PART B

UNITED STATES

OVERVIEW

27. Federal agencies have authority to collect personally-identifiable information. The principal federal biometric schemes in the US are the Integrated Automated Fingerprint System (IAFIS) and the Automatic Biometric Identification System (IDENT). Databases at the federal and state level are 'interoperational' and integrated.[59]

a) IAFIS

28. The IAFIS is a FBI-maintained automated fingerprint identification and criminal history database. It contains a range of information: fingerprints; criminal histories; mug shots; physical characteristics such as height, weight and hair and eye colour; and aliases. The IAFIS also includes the fingerprints of current and former US military personnel and federal government employees. It is currently the largest biometric database in the world.[60]

b) IDENT

29. The IDENT is a system for storing and processing biometric, limited biographic and encounter-related information, administered by the Department of Homeland Security.[61] It includes the US-VISIT program, which collates biometric data from non-citizens seeking entry. Originally developed for immigration control purposes, the system is now used for 'national security, law enforcement, immigration, intelligence and other DHS mission-related functions.'[62]

---

[59] The FBI, Department for Homeland Security (DHS) and Department of Defence's biometric databases are interoperable allowing free exchange of data. State level databases are integrated with those at the federal level in so far as all fingerprint and DNA data is shared with the FBI directly, and in certain limited instances with the DHS.

[60] See generally FBI, 'Integrated Automated Fingerprint Identification System', <http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis> accessed 21 February 2013.

[61] The data stored include, but are not limited to: fingerprints, photographs, name, date of birth, nationality, and other personal descriptive data and the context of the interaction with an individual including but not limited to location, document numbers, and/or reason information collected. See generally DHS, 'Privacy Impact Assessment for the Automated Biometric Identification System', <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf> accessed 21 February 2013.

[62] Department for Homeland Security, 'Privacy Impact Assessment for the Automatic Biometric Identification System (IDENT), 31 July 2006 (an overview of the IDENT system is provided at 2-4).

c) Other

30. In addition, each state has its own biometric database and a DNA database.[63] Fingerprinting is pervasive and is required by numerous state and federal laws across a range of non-criminal contexts, such as federal securities law[64] and laws concerning employment in bartending[65] and day-care.[66]

LEGAL FRAMEWORK

a) Overview

31. The Supreme Court has held that privacy interests are protected under the 1st, 4th and 14th Amendments of the Constitution.[67] States have also recognised a qualified right to privacy, expressly or impliedly.[68]

32. The US is considered to be an outlier among developed countries, as it does not have comprehensive data privacy legislation applying to both the public and private sector.[69]

33. At the federal level, the key piece of legislation is the Privacy Act 1974,[70] a federal statute placing general safeguards on information processed and held by the federal government.[71] This is supplemented by Guidance[72] and Privacy Impact Assessments.[73]

34. A huge number of additional federal and state statutes relate to individual privacy rights in discrete areas.

---

[63] J Lynch, 'From Fingerprints to DNA: Biometric Data Collection in US Immigrant Communities and Beyond' (Immigration Policy Centre 2012) 6 < https://www.eff.org/document/fingerprints-dna-biometric-data-collection-us-immigrant-communities-and-beyond> accessed 21 February 2013.
[64] 15 USC § 78q(f)(2) (2006).
[65] *See Iacobucci v City of Newport*, 785 F2d 1354 (6th Cir 1986) (a city ordinance requiring employees at places where liquor is served to be fingerprinted by the police was not unconstitutional, discussed further below).
[66] See California Health and Safety Code § 1596.871(a), (b)(1)(A)-(D), (c)(1) (2006).
[67] See *Katz v United States*, 389 U.S. 347 (1967), *Griswold v Conneticut,* 381 US 479, 85 S. Ct. 1678 and *Stanley v Georgia*, 394 U.S. 557 (1969).
[68] <http://www.ncsl.org/default.aspx?tabid=13467> explaining that constitutions in 10 states expressly recognise the right to privacy, while the highest courts of other states have established constitutional privacy rights.
[69] See Graham Greenleaf, 'The influence of European data privacy standards outside Europe: implications for globalization of Convention 108' (2012) 2 International Data Privacy Law 68, 70.
[70] 5 USC § 552a (2006).
[71] It applies only to data processing by the federal government and not to state governments or to the private sector.
[72] Department of Defence Privacy Program, DoD 5400.11-R, May 2007.
[73] Above n 63.

b) Safeguards under the Privacy Act 1974

35. The Act requires federal agencies, as data collectors, to adopt minimum standards for the collection, use, maintenance and dissemination of personal records.[74] However, the statute has been criticised for failing to provide sufficiently robust protection, particularly in relation to biometrics.[75] The establishment of a separate commission to ensure oversight of the Privacy Act was resisted. The act thus fell under the purview of the Office of Management and Budget and implementation has been deemed unsatisfactory.[76] The Act's main requirements are explained below.

i) No disclosure without consent (subject to significant exceptions)

36. Federal agencies are prohibited from disclosing any record, 'except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.'[77] However, this general rule is subject to 12 enumerated exceptions.[78]

ii) Individual right of information and access

37. The data subject must be informed of: the authority authorizing data collection; whether disclosure is mandatory or voluntary; the purposes of use of the data; and the effects the data subject will face for non-provision of the information.[79] The Act also requires federal agencies to grant access to the data subject and provide an opportunity to correct any errors in the information.[80] The agency must then either

[74] 5 USC § 552a(a)(4): The Act defines 'record' as: 'any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or photograph.' Although the Act does not specifically mention 'biometrics' it seems quite clear that the term 'record' can include biometric applications.

[75] LK Donohue, 'Technology Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age' (2012) 97 Minn L Rev 407, esp 468-476.

[76] J Slemmons Stratford & J Stratford, 'Data Protection and Privacy in the United States and Europe' (1998) IASSIST Quarterly, esp 18.

[77] 5 USC § 552a(b).

[78] ibid. While the exceptions are quite extensive, there are some safeguards built in. For example, the federal agency can disclose a record to another federal agency for civil or criminal law enforcement purposes, but only, 'if the head of the industry or instrumentality has made a written request to the agency which maintains the record specifying the particualr proportion desired and the law enforcement activity for which the record is sought.' The agency is also required to keep an accurate accounting of disclosures made.

[79] 5 USC § 552a(e)(3).

[80] 5 USC § 552a(d)(1).

correct the portion of the record or notify the individual of its refusal to do so (in which case there is an appeals process to be followed)[81] within 10 days.[82]

iii) Relevant and necessary information

38. The agency shall maintain, 'only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomophlished by statute or executive order'.[83] Further, information should be collected directly from the individual, 'to the greatest extent practicable'.[84]

iv) Data safeguarding

39. 'Appropriate administrative, technical, and physical safeguards' are required 'to insure the security and confidentiality of records and to protect against anticipated threats or hazards to their security or integrity.'[85]

CASE LAW

40. We are unaware of any cases, outside the criminal context, in which the collection and storage of biometric data has been challenged. However, the case-law below may offer some guidance.

41. In personal data cases, the Court tends to adopt a 'rational basis' review, asking whether the government has demonstrated a 'legitimate aim' and a 'rational connection' between the aim and the means used.[86] However, there is a suggestion that heightened scrutiny may apply where the personal data is especially sensitive.[87]

a) Informational privacy: constitutional challenges

i) Whalen v Roe (US Supreme Court) (1977)[88]

42. New York Statutes required physicians to report details of patients to whom they had prescribed certain drugs. The details were stored by the New York State

[81] 5 USC § 552a(d)(2)(B).
[82] 5 USC § 552a(d)(2)(A).
[83] 5 USC § 5552a(e)(1).
[84] 5 USC § 552a(e)(2).
[85] 5 USC § 552a(e)(10).
[86] *Iacobucci v City of Newport, Ky*, 785 F 2d 1354 (1986).
[87] *Doe v Attorney General*, 941 F2d 780 – Court of Appeals, 9th Circuit, 1991: 'the more sensitive the information, the stronger the state's interest must be'.
[88] *Whalen v Roe*, 429 US 589, 97 S Ct 869, 51 L Ed 2d 64.

Department. A group of patients and doctors challenged the statute on privacy grounds. The Supreme Court held the program did not pose a sufficiently serious threat to privacy to constitute a privacy violation.

43. Firstly, the Court recognised that the right to privacy included, 'an individual interest in avoiding disclosure of personal matters'.[89] Second, the Court concentrated on the 'orderly and rational' legislative process behind the New York statute.[90] Thirdly, the Court paid attention to the steps the agency had taken to prevent unauthorised disclosures of information. This enabled it to conclude that the statutory scheme 'evidence[d] a proper concern with, and protection of, the individual's interest in privacy.'[91]

44. Finally, the Supreme Court did express general concerns about privacy and emerging technologies. Mr Justice Stevens remarked,

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerised data banks or other massive government files[92]

45. Equally, Mr Justice Brennan, in a concurring opinion said,

> The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.[93]

ii) US v Westinghouse (US Court of Appeals, 3rd Cicruit) (1980)[94]

46. A subpoena granted to a health and safety inspector mandating an employer to disclose its employees' medical records was challenged as a violation of their constitutional right to privacy. The US Court of Appeals held there was no violation since: the material contained in the medical records was not 'sensitive';[95]

---

[89] ibid Stevens J at 599.
[90] ibid Stevens J at 597: 'The New York Statute challenged in this case represents a considered attempt to deal with such a problem. It is manifestly the product of an orderly and rational and legislative decision. It was recommended by a specially appointed commission which held extensive hearings on the proposed legislation, and drew on experience with similar programs in other states.'
[91] ibid Stevens J at 605.
[92] ibid.
[93] ibid 607.
[94] *US v Westinghouse*, 638 F 2d 570.
[95] ibid 579.

effective security arrangements were in place;[96] and there was a strong public interest in allowing the health and safety inspector to have access to the medical records in this case.

47. The Court of Appeals held:

> The factors that should be considered in deciding whether an intrusion into an individual's privacy is justified are the type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorised disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognisable public interest militating toward access.[97]

48. Again, the Court issued a cautionary note about large scale data protection systems:

> Proliferation in the collection, recording and dissemination of individualised information has made the public, Congress and the judiciary increasingly alert to the threat such activity can pose to one of the most fundamental and cherished rights of American citizenship, falling within the right characterisd by Justice Brandeis as "the right to be let alone"… Much of the concern has been with the governmental accumulation of data and the ability of government officials to put information technology to uses detrimental to individual privacy, which have been facilitated by the spread of data banks and by the increasing storage in computers of sensitive information relating to the personal lives and activities of private citizens.[98]

b) Fingerprinting: constitutional challenges in the non-criminal context

i) Thom v New York Stock Exchange (Dist. Court, SD New York) (1969)[99]

49. A law requiring the fingerprinting of employees belonging to firms that carried out security exchanges was challenged on multiple grounds, including invasion of privacy. In a state level court, Edward Weinfeld DJ propounded a 'rational basis' test:

> The state having presented a valid justification…for the original taking of the prints under reasonable circumstances, their use for future identification purposes, even in criminal investigations, is not impermissible.[100]

---

[96] ibid 579-580.
[97] ibid 578. Also note *Doe v Attorney General* (n 87): 'the more sensitive the information, the stronger the state's interest must be.'
[98] ibid 576.
[99] *Thom v New York Stock Exchange*, 306 F Supp 1002 (1969).

ii) Iacobucci v City of Newport, Ky (US Court of Appeals, 6th Circuit) (1986)[101]

50. A city ordinance requiring employees, at places where liquor is served, to be fingerprinted by the police was found to be constitutional. Martin CJ, citing *Thom* (above), reasoned that, 'the ordinance bears a rational relationship to a legitimate governmental interest, we view it as a proper exercise of the City's police power'.[102]

51. He then went on provide a hierarchy of protected personal information:

> Whatever the outer limits of the right to privacy, clearly it cannot be extended to apply to a procedure the Supreme Court regards as only minimally intrusive Enhanced protection has been held to apply only to such fundamental decisions as contraception…and family living arrangements. Fingerprints have not been held to merit the same level of constitutional concern.

[100] ibid 1011.
[101] Above n 86.
[102] ibid 1355.

ISRAEL

OVERVIEW

52. The Law for Including Biometric Identifying Means and Data in Documents of Identification and in Databases 2009 (the Biometric Indentification Law) was passed by the Knesset of Israel in December 2009. It provides for the embedding of biometric data (fingerprints and computerized tags of facial features) in Israeli IDs and passports, and allows for the creation of a database containing biometric data on all Israeli citizens. In addition, the data would be used by the Ministry of Interior in its future plans to create forgery-proof identification papers and passports, and allow Israeli security forces to identify and locate individuals suspected of criminal activity.

53. Despite its rhetorical appeal, opponents of the law — which includes prominent Israeli scientists and security experts — have warned that the existence of such a database risks damaging both civil liberties and state security, as any leaks could be used by criminals or hostile individuals against Israeli residents.[103]

LEGAL FRAMEWORK

54. Under Israeli law, privacy is protected by both the Basic Law: Human Dignity and Liberty 1992 (Basic Law) and the Privacy Protection Act 1981 (PPA). The Basic Law stipulates in section 7(a) that 'all persons have the right to privacy', although the right to privacy is not explicitly defined. Section 7(b)-(d) goes on to provide specific instantiations of that right:

> (b) There shall be no entry into the private premises of a person who has not consented thereto;
> (c) No search shall be conducted on the private premises of a person, nor in the body or personal effects;
> (d) There shall be no violation of the confidentiality of conversation, or of the writings or records of a person.

[103] Avner Pinchuk, 'The Campaign Against the Biometric Database Act' (The Public Voice Civil Society Meeting, Jerusalem, 25 October 2010) <http://thepublicvoice.org/eventsisrael10/Avner_Pinchuk_ACRI_TPV_Meeting_Jerusalem_10_25_10.pdf> accessed 21 February 2013.

55. The Israeli Supreme Court, in several key decisions,[104] has stressed that the right to privacy is a basic constitutional right; however, just like all other fundamental rights, the right to privacy is not absolute. It is subject to the 'limitations clause' in section 8 of the Basic Law, which states: 'There shall be no violation of rights under this Basic Law except by a law befitting the values of the State of Israel, enacted for a proper purpose, and to an extent no greater than is required.' These protections have effects similar to the legitimacy of purpose and proportionality tests in the European human rights and Data Protection law. Any executive or legislative action, such as the biometric database initiative, would thus be subject to this constitutional instruction.

56. The PPA forms the main element of Israeli data protection law, although it too does not define the right to privacy.[105] The PPA applies to both the private and public sector, and sets out administrative, civil, and criminal rights and obligations. Chapter 1 deals with general privacy protection: section 1 prohibits infringement of individual's privacy without that individual's consent; section 2 deals with general privacy protections, listing eleven alternative causes of action for infringement of privacy. Especially pertinent in the context of the biometric database is section 2(9): 'using, or passing on to information on a person's private affairs, otherwise than for the purpose for which it was given' (exempt from liability for 'security services'). Chapter 2 establishes a procedure for database registration, and sets forth information privacy principles which include: transparency; security; purpose limitation; confidentiality; access and rectification; and restrictions on cross-border data flows.[106] Furthermore, it defines information as 'data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person.' This list, however, is not exhaustive; as the Supreme Court held in *State of Israel v Bank HaPoalim:*

> [T]he term 'information' must be interpreted in line with the legislative intent of the PPA. It should include data that can be derived from a database which is not indexed according to individual names. In other words...if financial data concerning an

[104] HCJ 4804/94 *Station Film Corporation Ltd. v Movie Censorship Committee*, 50(5) P.D. 661, 675; CA 4463/94, 4409/94 *Golan v Prison Service*, 50(4) P.D. 136.
[105] Students of the Interdisciplinary Law & Technology Workshop, *Privacy in the Digital Environment* (The Haifa Center of Law and Technology Publication Series, Publication No. 7, 2005) 7.
[106] Ian Bourne, 'A Guide to Data Protection in Israel' (The Israeli Law, Information and Technology Authority January 2010) <http://www.justice.gov.il/NR/rdonlyres/C7DE27A2-4CC2-4C5E-9047-C86CC70BD50B/18333/AguidetodataprotectioninIsrael1.pdf> accessed 21 February 2013.

individual can be derived from a database that is not indexed on a personal basis, it should be regarded as "information" under Section 7 of the PPA.[107]

57. In Israeli case law, there is no uniform definition of the right to privacy and its extent is unclear. Save for a few cases, case law has chosen not to define the right to privacy, but instead determines on a case-by-case basis whether the interests at hand form part of 'the right to privacy'.

CASE LAW

58. Since its passing, the Biometric Identification Law has drawn considerable criticism from its opponents. Most recently, in *Nahon v. Knesset*,[108] the High Court of Justice responded to a petition drafted by the Association of Civil Rights in Israel (ACRI) and the Digital Rights Movement, challenging the Biometric Identification Law and a proposed two-year 'pilot' programme.[109] The petition itself was not directed against either the use of 'smart' ID cards or the intent to embed them with biometric data; rather, it condemned the compiling of biometric identification methods and data into one central databank.[110] The Court ultimately dismissed the petition as premature, given that the pilot programme had not yet been implemented. However, the Justices strongly criticised the proposed scheme during the hearing, leading the Interior Ministry to give assurances that it would explore other options.

59. The petitioners maintained that a biometric identification system should be able to work without a central database. A central databank is neither necessary nor intended for preventing the forging of identification papers. For instance, to prevent forgeries, it would be sufficient to issue ID cards with an electronic chip (like credit cards).[111] In addition to proposing alternative solutions, the general argument was this: a databank that stores biometric data on all Israeli residents is a

---

[107] CA 86/89 *State of Israel v Bank HaPoalim*, 24(2) PD 726, 731, para 10 (5750/51-1990) as translated by Bourne (n 4).

[108] HCJ 1516/12 *Nahon v Knesset* S.CT 842 (2012) (judgment available in Hebrew) <http://elyon1.court.gov.il/files/12/160/015/c03/12015160.c03.htm> accessed 21 February 2013.

[109] Rawlson King, 'Israeli jurists right to call biometric database "extreme" and "harmful"' *BiometricUpdate.com* (30 July 2012) <www.biometricupdate.com/201207/israeli-jurists-right-to-call-biometric-database-extreme-and-harmful/> accessed 21 February 2013.

[110] The Association for Civil Rights in Israel, 'Introduction from ACRI Petition to the High Court of Justice: Objections to a Governmental Biometric Database' (February 2012) <http://www.acri.org.il/en/wp-content/uploads/2012/02/biometric.pdf> accessed 21 February 2013.

[111] ibid.

sensitive and powerful resource that has the potential to become an unparalleled mechanism for surveillance and control, resulting in both direct and indirect breaches to constitutional rights (e.g. right to dignity, liberty and privacy).

60. During the hearing, the Justices of the High Court were harshly critical of the Israeli's government biometric scheme. In particular, they were not convinced that the government would have to maintain a central database given that smart identification cards can be issued without one.[112] Given the other security infractions that have occurred with Israeli biometric systems in the past (e.g. theft of biometric data for nine million Israeli citizens in 2006), the High Court demanded that the Interior Ministry rework its planned pilot of the program to evaluate whether it is actually *necessary* to store the population's biometric data in a single, centralized database. Since then, the Interior Ministry has been exploring other options, as well as evaluating safeguards to limit the possibility of data leaks and information theft.[113]

61. Other cases, of particular relevance to the biometric data scheme, include the following:

    a. In *Plonit (Jane Doe) v National Rabbinical Court* (2006), the Israeli Supreme Court held that the right to privacy is not only one of the most important fundamental rights, but it plays a vital role in shaping the democratic character of Israel's legal system. These decisions were reiterated in *Rami Mor v Barak ETC* (2010)—a case in which the Supreme Court refused to order that an Internet service provider unmask a John Doe defendant — by holding that the constitutional right to privacy entails a right *to anonymity*.[114]

    b. In *Association for Civil Rights in Israel v Minister of Interior* (2004), the Israeli Supreme Court ruled that the data sharing practices within the public sector, while authorized by statute, were unconstitutional. The data transfers were considered overly broad, which in turn had a disproportionate effect on an individual's privacy rights. The court ruled that data transfers must be restricted by regulations specifying the uses of data, its users and security measures.

[112] King (n 109).
[113] The Association for Civil Rights in Israel (n 110).
[114] LCA 4447/07 *Rami Mor v. Barak E.T.C the Company for Bezeq International Services Ltd* (2010) as translated by Google Translate < http://elyon1.court.gov.il/files/07/470/044/p10/07044470.p10.htm> accessed 21 February 2013.

Moreover, it specified that the transfer of data between government officials and private sector financial institutions must be authorized explicitly through primary legislation; in this case, anti-money laundering provisions in secondary regulations did not suffice.[115]

[115] HCJ 8070/98 *ACRI v Ministry of Interior*, 58(4) S.CT 842 (2004) as translated by Google Translate <http://elyon1.court.gov.il/files/98/700/080/L09/98080700.l09.htm>.

AUSTRALIA

OVERVIEW

62. The Australian Constitution does not contain a right to privacy, or any similar right, and no such rights have been found to be implied in the Constitution. There is no federal bill of rights and no general right to privacy has been recognised in the common law. As a result, privacy is protected through legislation, principally the Privacy Act 1998 (Privacy Act).

63. Legislation to create a national identity system — the 'Australia Card' — which would have amalgamated all government identification systems into a single database, was introduced in the 1980s, but abandoned due to strong public opposition.[116] No subsequent government has shown serious interest in revisiting the concept and even comparatively limited proposals, such as a consolidated healthcare access card, have been rejected. Specific biometric systems are widely used by the government, such as for 'ePassports', and by private bodies, such as nightclubs, which collect biometric information as a condition of entry, typically for the purpose of identifying troublemakers.[117] The Privacy Act regulates these systems.

LEGAL FRAMEWORK

64. The principal protection for privacy in Australia is the Privacy Act. It operates alongside a set of overlapping, complex and potentially contradictory[118] federal and state/territory statutes that address specific aspects of privacy law, such as telecommunications.

65. The Privacy Act was introduced in order to implement the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and Australia' s obligations under Article 17 of the International Covenant on Civil and Political

[116] Graham Greenleaf, 'The Australia Card – deux ex machine?' (1998) 3(6) Computer Law & Security Report 6.
[117] Biometrics Institute, 'Where are biometrics used' <http://www.biometricsinstitute.org/pages/faq-3.html> accessed 21 February 2013.
[118] Australian Law Reform Commission, 'Review of Australian Privacy Law, Discussion Paper No 72 '(2007) 328–9.

Rights.[119] It was initially designed only to protect personal information in the possession of federal government departments, but was subsequently extended to apply information in the possession of most private parties.

66. The Privacy Act regulates how information is collected, used, disclosed and kept.[120] Government agencies must take reasonable steps to protect personal information against loss, unauthorised access, modification, use or disclosure, and other misuse. These obligations are expressed in general terms, for example to ensure that there are 'such security safeguards as it is reasonable'.[121] The Privacy Act requires that 'sensitive information' be managed with particular care. Sensitive information, generally, can only be collected with a person's consent and only disclosed for limited reasons.[122] In December 2012 biometric information was added to the list of material classified in the Privacy Act as 'sensitive information' by statutory amendment.[123] The list of 'sensitive information' also includes, among other things, information or opinion about a persons racial or ethnic origin, religious affiliations, philosophical beliefs, sexual preferences and criminal record.[124]

67. The operation of the Privacy Act is overseen by the Office of the Australian Information Commissioner (OAIC), an independent statutory body. While the OAIC has been active in investigating complaints, it has not considered a challenge to the existence of government databases containing personal information. It would not have the power to do so if such databases were established by legislation. The OAIC's function is limited to the specific powers granted to it under statute, which are to ensure that existing legislation is complied with, rather than to evaluate new legislation.[125]

---

[119] Office of the Australian Information Commissioner, 'History' <http://www.privacy.gov.au/aboutprivacy/history> accessed 21 February 2013.
[120] Privacy Act 1988, s 14.
[121] Privacy Act 1988, s 14 Principle 4.
[122] Privacy Act 1998, Schedule 3, National Privacy Principle 10.
[123] The amendment was made by the Privacy Amendment (Enhancing Privacy Protection) Act 2012, Schedule 1, s 42.
[124] Privacy Act 1998, s 6(1), 'sensitive information'.
[125] Australian Information Commissioner Act 2010, s 9.

CASE LAW AND POLITICAL DEBATE

68. There is no Australian case law in which a superior court has recognised a right to privacy in the Constitution or in the common law.[126] In *ABC v Lenah Game Meats* the High Court left open the possibility that such a right might develop in the common law,[127] but, even if it did, such a common law right could be overridden by legislation.

69. The OAIC, (and its predecessor the Australian Privacy Commissioner) investigates complaints about government and private bodies that may be in breach of the Privacy Act[128] and conducts audits of bodies that hold significant amounts of private data,[129] but its powers are limited to ensuring compliance with the existing legislation.

70. In 1985 the Australian Federal Government proposed a national identity card and associated database, which was intended to reduce benefit fraud, tax fraud and to control illegal immigration.[130] It ultimately abandoned the proposal in the face of sustained public opposition and criticism, primarily on privacy grounds.[131] In 2006 the Federal Government tabled legislation for a single health care and social services access card, to replace 17 existing government issued cards.[132] The bill was withdrawn in 2007 after a Senate inquiry harshly criticised the proposal on the basis of poor drafting and inadequate protections for privacy.[133] The inquiry expressed concern about the proposal generally:[134]

---

[126] *Victoria Park Racing & Recreation Grounds Co Ltd v Taylor* [1937] HCA 45; (1937) 58 CLR 479.
[127] *ABC v Lenah Game Meats Pty Ltd* [2001] HCA 63; 208 CLR 199. Such a right has been asserted in two lower state court decisions, but they have never been followed by higher courts: *Doe v ABC* [2007] VCC 281 and *Grosse v Purvis* [2003] QDC 151.
[128] *For* example *J and Commonwealth Agency* [2011] AICmrCN 4.
[129] See for example Office of the Australian Information Commissioner, Audit of the National Document Verification Service, Centrelink, June 2011 <http://www.oaic.gov.au/publications/reports/audits/document_verification_service_audit_report.html> accessed 21 February 2013
[130] Australian Parliamentary Library 'Identity Cards and the Acceess Card,' 17 August 2010 <http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/Publications_Archive/archive/identitycards> accessed 21 February 2013
[131] Greenleaf (n 116) 6.
[132] Australian Parliamentary Library 'Identity Cards and the Acceess Card,' 17 August 2010 <http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/Publications_Archive/archive/identitycards> accessed 21 February 2013
[133] Senate Standing Committees on Finance and Public Administration, Report into the Human Services (Enhance Service Delivery) Bill 2007, 15 March 2007, see especially Chapter 3
[134] Senate Standing Committees on Finance and Public Administration, Report into the Human Services (Enhance Service Delivery) Bill 2007, 15 March 2007, 3.89

> The register gives rise to the prospect of the government having unprecedented access to a single national database containing the majority of Australia's adult population's basic personal information. It is seen as presenting a major risk to personal privacy and security, not only from government agencies but also other parties with malicious intent.
> …
>
> [In a historical context] [n]o previous Australian government, even in wartime, has effectively required all its citizens to give it a physical representation of themselves, nor contemplated having this stored in one national database

However, there was no suggestion that the Australian Parliament lacked the power to introduce the legislation, simply that it would be unwise to do so.

COUNCIL OF EUROPE

OVERVIEW

71. The European Court of Human Rights (ECtHR) adjudicates the compatibility with the European Convention on Human Rights[135] (ECHR) of Council of Europe Member States' national measures, including privacy legislation. The ECtHR therefore ensures that national biometric identification systems are consistent with the human rights norms enshrined in the ECHR, which include the right to respect for private life.

LEGAL FRAMEWORK

a) Article 8 ECHR

72. The legal framework for privacy protection under the jurisdiction of the ECtHR centres upon Article 8 ECHR. Article 8(1), so far as relevant, states that: 'Everyone has the right to respect for his private… life'.

73. Article 8(2) states:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

74. Article 8(1) ECHR therefore protects the right to privacy. Article 8(2) lists exhaustively the circumstances in which limitations on the right may be considered justified. The right can be limited in pursuance of a number of legitimate aims which may be relied on by a public authority acting in accordance with law and only so far as is necessary in a democratic society. It is for the public authority in each case to demonstrate that the measure which constitutes an interference with the

[135] Convention for the Protection of Human Rights and Fundamental Freedoms 1950.

right to private life is in accordance with law, serves a legitimate aim and is proportionate to the achievement of that aim.[136]

b) Data Protection Convention

75. The Council of Europe has also produced a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Data Protection Convention).[137] The ECtHR is not entitled to interpret this Convention as it is entitled to interpret the ECHR, however the Court does refer to the Data Protection Convention in its case law to guide its interpretation of the notion of private life in Article 8 ECHR. The purpose of the Data Protection Convention is to extend the safeguards of the right to privacy in relation to personal data undergoing automatic processing.[138] 'Personal data' is defined in the Data Protection Convention as 'any information relating to an identified or identifiable individual'.[139] The Explanatory Report[140] clarifies that 'automatic data processing' is capable of a flexible interpretation[141] and includes electronically processed data, but not data which is merely collected.

76. States Parties have a duty to take the necessary measures in their domestic legislation to give effect to the principles of data protection set out in the Convention in order to ensure respect in their territory for the fundamental human rights of all individuals as regards the processing of personal data.[142] For example, sensitive data may not be processed automatically unless domestic law provides appropriate safeguards. The categories of sensitive data under the Convention include personal data 'revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life [and]… relating to criminal convictions'.[143] States must take appropriate security measures for the protection of personal data stored in automated data files.[144]

---

[136] On the application of proportionality in the context of Article 8 ECHR, see Harris, O'Boyle and Warbrick, *Law of the European Convention on Human Rights* (2nd edn, OUP 2009) Ch 9, 407-422.
[137] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 (Data Protection Convention).
[138] ibid Preamble.
[139] ibid art 2(a).
[140] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 – Explanatory Report <http://conventions.coe.int/Treaty/EN/Reports/HTML/108.html> accessed 21 February 2013.
[141] ibid [31].
[142] Data Protection Convention, art 4.
[143] ibid art 6.
[144] ibid art 7.

77. The Explanatory Report expounds that the principles enshrined in the Data Protection Convention are intended to be universal and not limited to a European context.[145] The ECtHR refers to the Data Protection Convention in its case law to assist with the interpretation of the right to respect for private life under Article 8 of the ECHR.

CASE LAW

78. The landmark ECtHR case on the retention of biometric information and the right to respect for private life is *S and Marper v United Kingdom*.[146]

79. The applicants were arrested and charged with criminal offences. Fingerprints and DNA samples were taken from them under section 64 of the Police and Criminal Evidence Act 1984. One of the applicants was acquitted and the case against the other was discontinued. The applicants requested the destruction of their fingerprints, cellular samples and DNA profiles held by the police, but this was denied. At national level, the House of Lords rejected the applicants' appeal against the decision not to destroy the data.[147] The applicants complained to the ECtHR that the retention of their fingerprints, cellular samples and DNA profiles after the acquittal/discontinuance of their case was inconsistent with the right to respect for private life enshrined in Article 8 ECHR.

80. The Grand Chamber of the ECtHR held that the concept of 'private life' is a broad term, not susceptible to exhaustive definition, and includes means of personal identification.[148] All forms of information retained in the instant case were held to fall within the meaning of 'personal data'.[149] The Court concluded that retention of each type of data amounted to an interference with the right to respect for private life under Article 8 ECHR.[150]

81. Given the nature and amount of personal information contained in the cellular samples, their retention per se was regarded as interfering with the right to respect

---

[145] Data Protection Convention Explanatory Report [24] and [90].
[146] *S and Marper v UK* (2009) 48 EHRR 50.
[147] *R (on the application of S) v Chief Constable of South Yorkshire* [2004] UKHL 39, [2004] 1 WLR 2196.
[148] *S and Marper* (n 146) [66].
[149] ibid [68].
[150] ibid [73], [75] and [86].

for the private lives of the individuals.[151] The DNA profiles, as sensitive data containing much information relating to personal identification, revealing racial origin or matters of health, attracted a heightened level of protection.[152] As regards retention of fingerprint data, the Court revisited prior ECHR jurisprudence. Whether the taking of fingerprints constituted an interference with the right to respect for private life was left open in *McVeigh*.[153] In *Kinnunen v. Finland*[154] the European Commission on Human Rights held that retention did not constitute an interference with the Article 8 right. However, the ECtHR considered it appropriate to review this issue in light of subsequent developments in the law relating to the processing of photographs[155] and voice sample data.[156] In relation to retention of photographs, the holding in the *Friedl* case that there was no interference with the Article 8 right was based to a significant extent on the fact that the photographs were not entered into any data processing system, which suggests that whenever photographs are retained and processed, there will be an interference with Article 8. The taking of voice samples by police in *PG v UK*[157] was held to constitute an interference with the right to respect for private life. The Court in *S and Marper* concluded that retention of fingerprints could in itself give rise to important private life concerns[158] and constituted an interference with the right to respect for private life.

82. These conclusions were ultimately reiterated and reinforced:

> [T]he mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data.[159]

The Court accepted that the retention of the applicants' fingerprint and DNA records had a clear basis in domestic law.[160] The Court also accepted that the

---

[151] ibid [72].
[152] ibid [76].
[153] *McVeigh, O'Neill and Evans v UK* (1983) 5 EHRR 71.
[154] *Kinnunen v Finland*, no. 24950/94, Commission decision of 15 May 1996.
[155] *Friedl v Austria* (1996) 21 EHRR 83.
[156] *PG v UK* (2008) 46 EHRR 51.
[157] (2001) 31 EHRR 1016.
[158] *S and Marper* (n 146) [85].
[159] ibid [121].
[160] ibid [97].

retention of fingerprint and DNA data pursed the legitimate purpose of the detection and prevention of crime[161].

83. However, the ECtHR held that the interference with the right to respect for private life by the retention of this data was not justifiable as necessary in a democratic society[162]. The Court referred to the importance of the privacy interest in data protection:

> The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private… life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article. The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned… The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored. The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse…

The intrinsically private character of the information taken from the applicants called for the Court to exercise careful scrutiny of State measures relating to the retention and use of such data.

84. The Court placed weight on the fact that the UK was the only Member State of the Council of Europe which permitted indefinite retention of fingerprint and DNA data.[163] It compared the practice of the majority of other Member States, which required such samples to be removed or destroyed either immediately or within a certain time after acquittal or discharge.[164] The blanket and indiscriminate nature of its powers of retention meant that the UK had overstepped its margin of appreciation and failed to strike a fair balance between the competing public and private interests. Accordingly, the retention of the applicants' data was a disproportionate interference with their right to respect for private life and a constituted a violation of Article 8 ECHR.[165]

---

[161] ibid [100] and [117].
[162] ibid [125].
[163] ibid [110].
[164] ibid [108].
[165] ibid [125].

85. The Grand Chamber's approach in *S and Marper v UK* therefore indicates that a national system of collection and retention of biometric information must incorporate sufficient safeguards in order adequately to protect the right to respect for private life. It appears that by 'appropriate safeguards', the Court means that the law must include requirements against indefinite storage and that retention must not be excessive in terms of coverage, i.e. overly inclusive as regards whose data is to be stored.

EUROPEAN UNION

OVERVIEW

86. The European Union has enacted Council Regulation (EC) 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.[166] This was amended by Council Regulation (EC) 444/2009 of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel document issued by Member States. This introduces passports and travel documents that contain biometric data, namely facial image and two fingerprints taken flat in interoperable formats.[167]

LEGAL FRAMEWORK

a) Charter on Fundamental Rights of the European Union

87. The Charter has the same legal value as the Treaties.[168] Article 7 guarantees respect for private and family life and Article 8 guarantees the protection of personal data. Limitations may be imposed on Articles 7 and 8, as long as the limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest.[169]

b) European Convention of Human Rights (ECHR)

88. The rights in the ECHR, including Article 8,[170] constitute general principles of Union law.[171] Also, where Charter rights correspond to Convention rights, the meaning and scope of those rights are to be the same as those laid down by the Convention[172] and nothing in the Charter is to be interpreted as restricting or adversely affecting the rights recognised by the Convention.[173]

---

[166] Regulation 2252/2004 of 13 December 2004 [2004] OJ L385/1.
[167] ibid art 1(2).
[168] Treaty on European Union, art 6(1).
[169] Charter on the Fundamental Rights of the European Union, art 52(1).
[170] Which protects the right to respect for private and family life, home and correspondence. See above para 72-75.
[171] Treaty on European Union, art 6(3).
[172] Charter on Fundamental Rights of the European Union, art 52(3).
[173] ibid art 53.

c) Council Directive 95/46/EC[174]

89. The Directive deals with 'personal data' which is defined in Article 2(a) as 'any information relating to an identified or identifiable natural person'. The Working Party,[175] which gives opinions to the European Commission on Union laws affecting the right to privacy, has concluded that biometric data would fall into this category since '[i]n the context of biometrical identification, the person is generally identifiable, since the biometric data are used for identification or authentication/verification at least in the sense that the data subject is distinguished from any other.'[176]

90. Article 8 provides extra safeguards for 'sensitive data', defined as data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and … health or sex life'.[177] The Working Party identifies that biometric systems could classified as 'sensitive information' where the system is based on face recognition, which would reveal ethnic or racial origin.[178]

91. Together Article 6(1)(b) and 6(1)(c) require that the collection of data should be tightly linked to the purpose and should not be excessive in relation to the purpose. However, Article 13 does allow for derogation from this, and other specified obligations and rights.[179]

92. The Preamble and Article 1(1) state that the right to privacy is to be respected. The safeguards provided for, give a number of rights to the data subject, including the right to information[180], right of access[181] and right to object[182]. There are guarantees

[174] Council 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 [1995] OJ L281/31.
[175] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, which was set up by section 29 of Directive 95/46. The Working Party is comprised of representatives from data protection authorities in all EU Member States, the European Data Protection Supervisor, and a representative of the EU Commission.
[176] Working Party, 'Working Paper 80: Working document on biometrics' (2003) 12168/02/EN [section 3.1]
[177] Council Directive 95/46/EC, art 8(1).
[178] Working Party, 'Working document on biometrics' (n 176) 10.
[179] Allows derogations from Articles 6(1), 10, 11(1), 12 and 21 of Directive 95/46
[180] Council Directive 95/46/EC, arts 10 and 11.
[181] ibid art 12.
[182] ibid arts 14 and 15.

relating to data quality[183] and consent[184]. Also, the Directive lays down security measures[185], notification obligations[186] and prior checking.[187]

d) Council Regulation (EC) 2252/2004[188]

93. The two aims of the scheme, specified in Article 4(3), are to verify the authenticity of the document and the identity of the holder by means of directly available comparable features. This serves the overall aim of combating falsification and fraudulent use of passports and other travel documents issued by the Member States.

94. Recital 8 of the Preamble states that the protection for 'personal data' in Directive 95/46 still applies. There are extra safeguards provided in the Regulation. Article 1(2) provides that the data shall be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data. Article 4(1) gives a right to the data subject to verify and rectify, and Article 2 lays down technical specifications. The amendments in Regulation 444/2009 introduce Article 1a which requires qualified and authorised staff. The amendments also require compliance with international standards.[189]

CASE LAW AND POLITICAL DEBATES

95. Two Member States have referred questions to the European Court of Justice (ECJ) concerning the validity of Regulation 2252/2004. These are on the docket of the ECJ and are pending decision. The ECJ has not decided a case concerning biometric information before.[190] However, the ECJ has ruled on the right to the protection of personal data in general (noted below).

---

[183] ibid art 6.
[184] ibid art 7.
[185] ibid art 17.
[186] ibid art 18.
[187] ibid art 20.
[188] Council Regulation (EC) 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States [2004] OJ L385/1.
[189] This includes the ECHR, UN Convention on the Rights of the Child and the International Civil Aviation Organisation
[190] The ECJ has ruled on Regulation 2252/2004 before, in C-137/05 United Kingdom of Great Britain and Northern Ireland v Council of the European Union [2007] ECR I-11593, but this concerned the validity of the Regulation. The UK complained that the Regulation should be annulled because they did not take part in its adoption. The ECJ decided that the Regulation was valid. The specific issue of biometric data was not discussed.

a) Dutch preliminary reference

96. Firstly, the Dutch Council of State (*Raad van State*, the highest Dutch administrative court) referred the question to the ECJ whether the requirement of fingerprints in passports violates citizens' right to privacy.[191] This referral concerns four separate cases, where three Dutch citizens were denied passports and another citizen was denied an ID card for refusing to provide their fingerprints. The Dutch Council questions whether Article 1(2) of the Regulation is valid in the light of Articles 7 and 8 of the Charter, and Article 8 ECHR. They also question whether, if Article 1(2) is valid, this means that Article 4(3), in the light of Articles 7 and 8 of the Charter and Article 8 ECHR, must be interpreted as meaning that it should be guaranteed by legislation that the biometric data, must not be collected, processed and used for purposes other than the issuing of the document. This latter issue, concerning the purpose of the data, raises similar issues to that dealt with by the French Conseil Constitutionel.[192]

b) German preliminary reference

97. Secondly, a German Administrative Court (Gelsenkirchen District Administrative Court) has also referred a question to the ECJ concerning the Regulation.[193] This case involves a German citizen who was not issued a new passport because he refused to give his fingerprints. The German Court questions whether Article 2(1) is valid.[194]

c) C-139/01 Österreichischer Rundfunk and Others [2003] E.C.R. I-4989

98. The ECJ has decided cases on Directive 95/46 and the right to protection of personal data in general. Österreichischer Rundfunk concerned provisions of Austrian law which required public bodies subject to control by the Rechnungshof (Court of Auditors) to communicate to it the salaries and pensions exceeding a certain level paid by them to their employees and pensioners, together with the

---

[191] Case C-446/12 Reference for a preliminary ruling from the Raad van State (Netherlands), lodged on 3 October 2012 — W.P. Willems; other party: Burgemeester van Nuth; Case C-447/12 Reference for a preliminary ruling from the Raad van State (Netherlands), lodged on 5 October 2012 — H.J. Kooistra; other party: Burgemeester van Skarsterlân; Case C-448/12 Reference for a preliminary ruling from the Raad van State (Netherlands), lodged on 8 October 2012 — M. Roest; other party: Burgemeester van Amsterdam; Case C-449/12 Reference for a preliminary ruling from the Raad van State (Netherlands), lodged on 8 October 2012 — L.J.A. van Luijk; other party: Burgemeester van Den Haag.

[192] Décision n° 2012-652 DC du 22 mars 2012.

[193] Case C-291/12 Reference for a preliminary ruling from the Verwaltungsgericht Gelsenkirchen (Germany) lodged on 12 June 2012 — Michael Schwarz v Stadt Bochum.

[194] See further Germany, n 238 below.

names of the recipients. The ECJ held that the Directive had necessarily to be interpreted in the light of fundamental rights, in particular the right to privacy.[195] To establish an interference with the right to privacy, it was sufficient to find that data had been communicated by the employer to a third party.[196] The Court stated that 'the question was whether stating the names of the persons concerned in relation to the income received is proportionate to the legitimate aim pursued and whether the reasons relied on before the Court to justify such disclosure appear relevant and sufficient.'[197] The Court noted that there should be an examination as to whether the objective of keeping salaries within reasonable limits could have been attained effectively by transmitting the information as to names to the monitoring bodies alone. Similarly, the question arose whether it would have been sufficient to inform the general public only of the remuneration and other financial benefits to which persons employed by the public bodies concerned had a contractual or statutory right, but not of the sums which each of them actually received during the year in question.[198] However, the ECJ did not reach a final conclusion and the issue was left up to the Member State to decide.[199]

99. This case was followed by the ECJ in Joint cases C-92/09 and C-93/09 Volker und Markus Schecke GbR v Land Hessen; Eifert v Land Hessen;[200] where the ECJ stated that '[i]n relation to proportionality, derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.'[201]

[195] C-139/01 Österreichischer Rundfunk and Others [2003] E.C.R. I-4989 [68].
[196] ibid [75]
[197] ibid [86]
[198] ibid [88]
[199] ibid [94]
[200] [2010] ECR I-nyr.
[201] Joint cases C-92/09 and C-93/09 Volker und Markus Schecke GbR v Land Hessen; Eifert v Land Hessen; [2010] ECR I-nyr [77].

UNITED KINGDOM

OVERVIEW

100. There is no general 'right to privacy' under UK law. As a result, the courts, using Article 8 ECHR as their basis, have striven to develop the common law to afford adequate protection to privacy interests.[202] In addition to this, there are a number of discrete statutes addressing a range of privacy concerns, the most relevant of which is the Data Protection Act 1998.[203]

101. Since the government's ultimately unsuccessful attempt to introduce an identity card scheme (complete with biometric data) in 2006, the legislative trend has shifted towards greater protection of sensitive information — a movement typified by the recent Protection of Freedoms Act 2012.

LEGAL FRAMEWORK

102. Although there is no overarching right to privacy in the UK, domestic judicial and legislative intervention and laws enacted at European level have begun to fashion a piecemeal protection of sorts. Article 8 of the ECHR, incorporated into UK law by the Human Rights Act 1998,[204] states that everyone has the right to respect for their private and family life. It is evident that in some circumstances this respect may be infringed by the collection and storage of biometric data. In such circumstances, those responsible for the storage must justify the interference in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime, or for the protection of the rights of others (as per the permissible limitations of the right in article 8(2) ECHR).

103. Further to this, the Data Protection Act 1998 regulates the storage and use of 'personal data', which the Act defines as data relating to a living individual who can be identified from those data, or from a combination of those data along with other

[202] See *Campbell v Mirror Group Newspapers Ltd* [2004] UKHL 22.
[203] Data Protection Act 1998 <http://www.legislation.gov.uk/ukpga/1998/29/contents> accessed 21 February 2013.
[204] Human Rights Act 1998 <http://www.legislation.gov.uk/ukpga/1998/42/contents> accessed 21 February 2013.

information which the data controller has, or is likely to have.[205] The Act applies to any individual or organisation that 'determines the purposes for which and the manner in which any personal data are, or are to be, processed'.[206] Schedule 1 of the Act outlines eight key features,[207] which must be considered by any such individual or organisation. The most relevant, for the purposes of biometric information, are that data must be fairly and lawfully processed,[208] obtained for one or more specified and lawful purposes,[209] not kept for longer than is needed for these purposes,[210] and stored with appropriate security.[211] Indeed, where the data concerned consists of information as to, inter alia, an individual's racial or ethnic origin, alleged criminal history, or physical or mental health, then it will be considered sensitive and deserving of an even higher level of protection in its processing and storage[212]. Exemptions from the Act are available in a number of circumstances, including when compliance with the Act would fetter crime prevention[213] or risk national security[214]. Further exemptions arise where the Act might hamper functions — whether of a public nature, conferred by enactment on any particular body, or carried out by government — that are designed to protect the public against maladministration, financial loss or malpractice.[215] Finally, data processors that process information for the purposes a public register may be exempted from the requirement to notify the Information Commissioner.[216]

104. In addition, the government has recently introduced the Protection of Freedoms Act 2012[217] 'to restore the rights of individuals in the face of encroaching state power, in keeping with Britain's tradition of freedom and fairness'. The Act regulates the destruction, retention and use of fingerprints, footwear impressions and DNA samples and tightens up the relatively weak protections, formerly offered in the Police and Criminal Evidence Act 1984. Notable safeguards within the 2012

[205] Data Protection Act 1998, Section 1(1).
[206] ibid.
[207] Data Protection Act 1998, Schedule 1, Part 1.
[208] ibid Schedule 1, Section 1.
[209] ibid Schedule 1, Section 2.
[210] ibid Schedule 1, Section 5.
[211] ibid Schedule 1, Section 7.
[212] ibid Schedule 3.
[213] ibid Section 29.
[214] ibid Section 28(1).
[215] ibid Section 31.
[216] ibid Section 17(4).
[217] Protection of Freedoms Act 2012 <http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted> accessed 21 February 2013

Act include: the requirement that fingerprints and DNA taken from a person arrested for or charged with a minor offence are destroyed following a decision not to charge or an acquittal; the availability of only limited grounds upon which periods of retention may be extended; and the appointment of a Commissioner for the Retention and Use of Biometric Material, with powers of review, including the power to order destruction of information where it is deemed that the criteria for extended retention have not been met. Although commentary on the Act's effectiveness must be necessarily tentative, due primarily to its infancy, its introduction represents an acceptance of the need to treat biometric information with particular sensitivity and shows a willingness on the part of the UK government to comply with the ruling of the ECtHR in *S and Marper v UK*, which considered that the UK's former policy of DNA retention constituted a 'disproportionate interference with the applicants' right to respect for private life'.[218]

105. Finally, there is an independent regulatory authority — the Information Commissioner's Office — that deals principally with oversight of the Data Protection Act 1998. The role of this body is to monitor organisations and individuals that collect, use and keep personal information and ensure that their procedures accord with the statutory requirements. The Commissioner has the power to initiate criminal prosecutions and can also pursue avenues of non-criminal enforcement, audit, and impose monetary penalties of up to £500,000 for statutory infringements.

CASE LAW AND POLITICAL DEBATE

106. The movement in favour of the UK identity card stems back to the late 1990s when Labour Minister Jack Straw first proposed the idea of 'citizen's access card'. Following the September 11th attacks in the USA and the July 7th attacks in London, the notion that ID cards could offer valuable assistance in the fight against terrorism grew in popularity. The momentum of this argument gradually faded, and by the time the Identity Card Act 2006 came into force it was being justified primarily on the grounds that it would combat identity theft, help prevent illegal

[218] *S and Marper v UK* (n 146) [125].

immigration, and help people to prove their identities more easily when travelling, opening bank accounts and renting property.

107. The enabling legislation gave the government considerable discretion as to how the scheme was to be implemented. The eventual model involved a physical card that linked back to the national identity database, which contained information such as photographs, national insurance numbers, dates of birth, addresses, and biometric information, such as fingerprints. The scheme was compulsory for non-EU migrants and workers in high-risk areas, but was, at least theoretically, voluntary for the general population. In effect, however, given that it was impossible to renew travel documents without registering on the database, the scheme was de facto compulsory for the vast majority.

108. By the time the bill had worked its way to Parliament, opposition from many quarters had hardened. For instance, the then Foreign Secretary, Jack Straw, warned that the pursuance of the ID card policy was "deeply flawed". Despite further notable objections, including the scheme being condemned as 'compulsion by the backdoor' in the House of Lords debates[219] and a report by the London School of Economics suggesting that the costs of such a scheme would be unsustainable[220], the Bill passed by a narrow margin.

109. From its inception, the scheme faced further resistance, with the Conservatives and Liberal Democrats promptly announcing their defiant opposition to it. A report produced by 'Liberty' - an independent campaigning organisation working to promote civil liberties and human rights - opposed the scheme for its far-reaching implications 'on the relationship between the individual and the state' and expressed concerns regarding the aggregating of information streams which, although potentially innocuous when kept apart, were significantly more intrusive when amalgamated[221]. Further challenges on privacy grounds came from the Information Commissioner, Richard Thomas, who cautioned that the introduction of identity cards 'fundamentally changed the relationship between state and

[219] House of Lords Debate <http://www.parliament.the-stationery-office.co.uk/pa/cm200506/cmhansrd/vo060213/debtext/60213-24.htm> accessed 21 February 2013.
[220] LSE, 'The Identity Report' <http://is.lse.ac.uk/idcard/identityreport.pdf> accessed 21 February 2013.
[221] Liberty's response to the draft bill <http://www.liberty-human-rights.org.uk/pdfs/policy04/id-card-draft-bill-response.pdf> accessed 21 February 2013.

citizen'[222]. The Commissioner also expressed worries about the digital trail that would be left by the central logging of every ID check and pointed out that the register could act as a detailed log of individuals' activities and transactions.

110. In light of the staunch and persistent criticism, it is, perhaps, unsurprising that the first bill to pass through Parliament under the new Conservative-Liberal Democrat coalition government, was one which entirely reversed the effects of the Identity Card Act 2006 for UK citizens - the Identity Documents Act 2010. The 2010 Act did, however, retain the scheme of biometric residence permits in place for non-EU nationals, although these permits continue to be issued pursuant to different legislation and the information gathered is not stored on the (now abolished) national identity register.

[222] ICO report into Identity Cards <http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/id_cards_bill_-_ico_concerns_october_2005.pdf> accessed 21 February 2013.

FRANCE

OVERVIEW

111. The right to privacy enjoys constitutional as well as statutory protection in France. The French constitutional court, the *Conseil Constitutionnel Français*, interprets Article 2 of the French Constitution as implicitly including the right to privacy ('*le droit au respect de la vie privée*') which extends to the protection of personal data.[223] France adopted a general data protection law, Act 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties,[224] long before the European Union Directive on data protection.[225]

LEGAL FRAMEWORK

a) Constitutional protection

112. The *Conseil Constitutionnel Français* (hereafter: *Conseil*) has the power to strike down laws of the Parliament incompatible with the Constitution. The *Conseil* mainly exercises *a priori* judicial review, i.e. before the final promulgation of laws. Since the 2007 constitutional reform, the *Conseil* can also strike down laws of Parliament that have already been promulgated if a regular court refers the constitutional question to the *Conseil*.

b) Statutory Protection

113. The Act 78-17 of 6 January 1978 on Data processing, Files and Individual Liberties set up an independent administration authority, the Commission nationale de l'informatique et des libertés (CNIL). The CNIL serves as the national data protection agency under the 95/46 EC Directive.[226] It issues opinions on legislation concerning data protection. The CNIL is discussed in further detail below.

---

[223] Article 2 of the Declaration (secod sentence): '*These rights are liberty, property, security, and resistance to oppression*.' It is worth highlighting that due to the ancient nature of the text, the majority of rights are intrepreted from abstract rights included in Article 2. Hence, the right to privacy enjoys the status of a ful-blooded constitutional right, it does not merely remain in a penumbra of other rights.

[224] The Act 78-17 of 6 January 1978 on Data processing, Files and Individual Liberties.

[225] See above paras 89-92.

[226] 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.

CASE LAW

114. This section discusses one recent high profile precedent and includes further decisions concerning the treatment of biometric information by law enforcement agencies.

a) Décision n° 2012-652 DC du 22 mars 2012[227]

115. MPs requested the *Conseil Constitutionel* to review the constitutionality of national identity card legislation that aimed to introduce a new ID card with an electronic chip that included biometric information (face image and fingerprints) and established a national database for this information.[228] The alleged aim of the law was to fight against identity fraud. The petition argued that the scheme breached the right to privacy. The *Conseil* struck down part of the law, namely its Article 5 and 10.[229]

116. The *Conseil* began by stating that 'the right to respect for private life; that accordingly, the collection, registration, conservation, consultation and communication of personal data must be justified on grounds of general interest and implemented in an adequate manner, proportionate to this objective.'[230] It scrutinised four aspects of the law: (a) the size of the database, that potentially covered the whole population; (b) biometric data, namely fingerprints as particularly sensitive data because of their immutable nature; (c) the means proposed to achieve the aim of the law; (d) the plurality of the ends that the database was to serve according to the law. The court found that the Act served a legitimate aim, i.e. fighting against identity fraud, though the scheme was to be found disproportionate. The *Conseil* found that on the one hand the databases was broad in coverage included particularly sensitive data, on the other hand police and other judicial authorities were explicitly granted access to the database in cases unrelated to the original purpose of the law, i.e. the prevention of fraud.[231] The *Conseil* found it disproportionate even though the consultation of the database was

---

[227] Official English translation available at <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/pdf/conseil-constitutionnel-105428.pdf> accessed 21 February 2013.
[228] Loi du 6 mars 2010 relative à la protection de l'identité. (Identity Protection Act).
[229] This decision also had another prong on the commercial, private use of the chip that was struck down on different grounds, and it is irrelevant for this issue.
[230] Décision n° 2012-652 DC du 22 mars 2012 [8].
[231] ibid [10]: 'that the technical characteristics of this database as defined by the contested provisions enable it to be consulted for purposes that other than the verification of an individual's identity.'

'for investigative requirements relating to certain offenses if authorized by the public prosecutor or the examining judge'.[232] It should be noted that the *Conseil* did not take issue with the creation of a population-wide biometric database per se.

117. It is worth mentioning that the CNIL, the national data protection agency, also scrutinised the legality of the national database.[233] The CNIL held the legislator to higher standard when finding the law to be a disproportionate restriction on the right to privacy. According to the CNIL the legislator did not use the least restrictive means to achieve the legitimate aim with the same efficiency, hence the scheme amounted to a disproportionate restriction of the right to privacy. The CNIL stipulated that the fight against identity fraud did not compel the government to set up such a broad-scale biometric database. It held that a one-way identification system ('match on card') would have been equally effective in achieving the aim. The *Conseil Constitutionel* therefore showed more deference to the legislature in this respect.

b) Database maintained by the police and further law enforcement agencies

118. The *Conseil Constitutionel* has reviewed a number of other databases from the perspective of the right to privacy. Among them there are two that explicitly deal with biometric information. According to the official commentary issued by the *Conseil Constitutionel*, there is a greater threat to the right to privacy where databases are run for private purposes and if the purpose served by database falls outside the scope of criminal offenses.[234]

i) Décision n° 2010-25 QPC du 16 septembre 2010

119. The database in issue was set up by a statute and contained the DNA of various criminal offenders.[235] The *Conseil* did not find the scheme to breach the constitutional right to privacy, but it found that the legislature struck a proportionate balance between the right to privacy and the public interest. First, it found that the scheme contained the same guarantees that are embedded in the

[232] ibid [3].
[233] *Note d'observations de la Commission nationale de l'informatique et des libertés concernant la proposition de loi relative à la protection de l'identité du 25 octobre 2011.*
[234] 'Commentaire Décision n° 2012-652 DC du 22 mars 2012 Loi relative à la protection de l'identité' *prepared and put on line by the Conseil Constitutionel* page 14.
[235] This database was named: *Fichier national automatisé des empreintes génétiques* (FNAEG).

general Data Protection legislation (itself mirroring the requisite safeguards of the EU Directive 95/46/EC); second it found the institutional guarantees were deemed sufficient. They are mostly as follows: the database being processed and supervised by the court as opposed to the government; clear definition of the range of criminal offences that entail the processing of the criminal offenders' DNA data; efficient guarantees of clearing the database of DNA data belonging to mere suspected persons; further use of the database being strictly confined to similar law enforcement purposes. The test the *Conseil* adopted in this case amounted to a level of strict proportionality scrutiny.[236]

120. Prior to this decision, the *Conseil* issued a similar opinion in the case of a database containing the data of sexual offenders that could be consulted by public authorities in assessing applications for jobs that involve a high level of security.[237]

[236] Décision n° 2010-25 QPC du 16 septembre 2010, 14.
[237] Décision n° 2004-499 DC du 29 juillet 2004 on the so called FIJAIS database.

GERMANY

OVERVIEW

121. In Germany, no constitutional challenge has arisen specifically in relation to a biometric identification scheme.[238] However, constitutional challenges have arisen in the context of the transfer of information collected through the national population census,[239] the online searching of computers by intelligence authorities,[240] the retention of telecommunications data[241] and automatic number plate recognition.[242] These constitutional challenges have been based either on the 'right to informational self-determination' or the 'right to the integrity and confidentiality of information technology systems', which have both been implied into the German Constitution ('*Grundgesetz*'), or on the right to secrecy of communications that is contained in Article 10(1) of the German Constitution.[243]

---

[238] Note however, that a recent challenge to the storage of biometric information in RFID chips in passports (namely, the right of a person to be issued a passport without his fingerprints being taken) was made in a case before the Gelsenkirchen District Administrative Court in Germany *('Verwaltungsgericht Gelsenkirchen')*. This case (*Verwaltungsgericht Gelsenkirchen, Beschluss vom 15. Mai 2012, Aktenzeichen 17 K 3382/07*) challenged the validity of Article 1(2) of Council Regulation (EC) No 2252/2004 of 13 December 2004, as amended by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 6 May 2009. The question of the validity of the regulation has since been referred to the Court of Justice of the European Union ('ECJ') for determination. See: InfoCuria - Caselaw of the Court of Justice, 'Reference for a preliminary ruling from the Verwaltungsgerickt Gelsenkirchen (Germany) lodged on 12 June 2012 – Michael Schwarz v Stadt Bochum (Case C-291/12)' <http://curia.europa.eu/juris/document/document.jsf?text=&docid=126045&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=963296> accessed 21 February 2013. See further European Union, above para 95.

[239] BVerfG 15 December 1983, *BVerfGE* 65, 1 – *Census Act Case ('Volkszählung')*, discussed in S Michalowski and L Woods, *German constitutional law: the protection of civil liberties* (Ashgate 1999) 120-123.

[240] German Federal Constitutional Court (*Bundesverfassungsgericht*) decision of 27 February 2008, reference number: 1 BvR 370/07, available at <http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html> (in German) and at <http://www.bverfg.de/en/decisions/rs20080227_1bvr037007en.html> (in English) accessed 21 February 2013. See also: BVerfG 27 February 2008, *BVerfGE* 120, 274 – *Online Computer Surveillance Case*, discussed in D Kommers and R Miller, *The Constitutional Jurisprudence of the Federal Republic of Germany* (3rd edn, Duke University Press 2012) 417.

[241] German Federal Constitutional Court (*Bundesverfassungsgericht*) decision of 2 March 2010, reference number: 1 BvR 256/08, available at <http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html> (in German) accessed 20 February 2013; see however German Federal Constitutional Court (*Bundesverfassungsgericht*) Press Office, 'Data retention unconstitutional in its present form' (Press Release No. 11/2010, 2 March 2010) <http://www.bverfg.de/pressemitteilungen/bvg10-011en.html> accessed 21 February 2013.

[242] German Federal Constitutional Court (*Bundesverfassungsgericht*) decision of 11 March 2008, reference number: 1 BvR 2074/05 and 1 BvR 1254/07 <http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr207405.html> (in German); see also G Hornung and C Schnabel, 'Data Protection in Germany II: Recent decisions on online searching of computers, automatic number plate recognition and data retention' (2009) 25(2) Computer Law & Security Review 115, 117-119.

[243] German Constitution (*Grundgesetz*), Article 10, <http://www.bundestag.de/htdocs_e/documents/legal/index.html> (in English) accessed 21 February 2013. Note

122. In addition, Germany has one of the strictest statutory frameworks for data protection in the European Union.[244]

LEGAL FRAMEWORK

a) Constitutional protection

123. A general right to privacy is not expressly stated in the German Constitution. However, the German Federal Constitutional Court has found that it is implied by the 'right to the free development of one's personality'[245] that is contained in Articles 2(1) and 1(1) of the German Constitution.[246] Article 2(1) states that:

> [e]very person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law.[247]

124. Article 2(1) has been interpreted as extending not only to a right to privacy *('Recht auf Privatsphäre')*[248] but also to a right to informational self-determination *('Recht auf informationelle Selbstbestimmung')*[249] and a right to the integrity and confidentiality of information technology systems *('Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme')*.[250] State action that restricts these rights is justified only if it has a legal basis and if it is proportional.[251] In addition, the Court has stressed that in determining the content and scope of the right in Article 2(1), the guarantee of human dignity in Article 1(1) must be taken into consideration.[252]

---

that this version of the German Constitution was translated by Professor C Tomuschat and Professor D Currie, and revised by Professor C Tomuschat and Professor D Kommers in coorperation with the Language Service of the German Federal Parliament (*Deutscher Bundestag*), and reflects the German Constitution as at October, 2010.

[244] Privacy International, 'Germany: Country Report' (1 January 2011) <https://www.privacyinternational.org/reports/germany> accessed 21 February 2013.

[245] This right is also sometimes described in English as the 'right to self-determination', or as an 'autonomous fundamental right'. See T Hoeren and A Rodenhausen, 'Constitutional Rights and New Technologies in Germany' in R Leenes, B Koops and P De Hert (eds), *Constitutional Rights and New Technologies: A Comparative Study* (Asser Press c2006).

[246] ibid 138.

[247] German Constitution (*Grundgesetz*) (n 243), Article 2(1).

[248] See BVerfG 26 April 1997, *BVerfGE* 90, 255, 260, discussed in R Leenes et al (n 245) 138-145.

[249] *Census Act Case* (n 239).

[250] *Online Computer Surveillance Case* (n 240).

[251] R Leenes et al (n 245) 138.

[252] German Constitution (*Grundgesetz*), Article 10.

125. As well as these implied rights, Article 10 of the German Constitution provides that restrictions on '[t]he privacy of correspondence, posts and telecommunications' may be ordered only pursuant to a law'.[253]

b) Statutory protection

126. In Germany, data protection rights are also provided for in a number of statutory instruments. The Federal Data Protection Law *('Bundesdatenschutzgesetz', 'BDSG')*, constitutes the main and general legal framework for the protection of personal data, and implements the general EU Directive 95/46/EC.[254] Compliance with the provisions of the Federal Data Protection Law is monitored by the Federal Commissioner for Data Protection and Freedom of Information *('Bundesbeauftragter für den Datenschutz and die Informationsfreiheit', 'BfDI')*.[255]

127. Special rules concerning specific technologies are also found in the Telecommunications Act *('Telekommunikationsgesetz', 'TKG')*[256] and the Telemedia Act *('Telemediengesetz', 'TMG')*.[257] In addition, all of Germany's 16 States *('Länder')* have their own specific data protection regulations that cover the public agencies of each state.[258]

CASE LAW

a) Census Act Case

128. The Court first developed the right to informational self-determination in the *Census Act Case*.[259]

i) The nature and purpose of the challenged legislation

129. A national census was to be held according to the National Census Act (1983). The intention behind the census was to obtain comprehensive statistical data regarding the population, in particular, demographic, social and economic information on

---

[253] German Constitution (*Grundgesetz*) (n 245), Article 10.
[254] Federal Data Protection Law *('BDSG')* <http://www.gesetze-im-internet.de/bdsg_1990/> (in German and English) accessed 21 February 2013; EU Council Directive 95/46/EC (n 174); R Leenes et al (n 245) 145.
[255] Federal Commissioner for Data Protection and Freedom of Information *('BfDI')* available at <http://www.bfdi.bund.de/Vorschaltseite_DE_node.html> (in German and English) accessed 21 February 2013.
[256] Telecommunications Act *('TKG')* available at <http://www.gesetze-im-internet.de/tkg_2004/> (in German) accessed 21 February 2013; Leenes ibid.
[257] Telemedia Act *('TMG')* available at <http://www.gesetze-im-internet.de/tmg/> (in German) accessed 21 February 2013; Leenes ibid.
[258] Leenes ibid.
[259] *Census Act Case* (n 239).

which the government could base future political and economic decisions. The National Census Act placed an obligation on every household to fill in and return a census form and provided for the possibility of different state agencies comparing and exchanging the collected data.[260]

ii) The nature and scope of the right to informational self-determination

130. The court found that the general right of personality in Article 2(1), in conjunction with the guarantee of human dignity in Article 1(1), gave rise to an implied right to informational self-determination. The Court described the right to informational self-determination as follows:

> Individual self-determination, however, presupposes – even under the conditions of modern information processing techniques – that the individual has the freedom to decide whether to perform or omit actions, including the possibility of acting according to this decision. A person who cannot safely tell what information about him regarding certain areas is known to his social environment, and cannot to some extent assess the knowledge of potential partners of communication, can be essentially inhibited in his freedom to make autonomous plans and decisions. … If someone is uncertain whether deviant behaviour will at any time be noted and as information interminably be stored, used or transmitted, he will try not to stand out by such behaviour. … *It follows that the free development of one's personality under the modern conditions of data processing presupposes the protection of the individual against unlimited collection, storage, use and transmission of his personal data*. This protection is therefore included in the basic right of Article 2(1) in conjunction with Article 1(1) of the Constitution. The basic right guarantees insofar the right of the individual to decide in principle about the disclosure and the use of his personal data (emphasis added).[261]

131. In determining what type of information was covered by the scope of the right, the Court considered that the need for information to be protected depended not only on its content, but also on its possible use.[262]

iii) Proportionality assessment

132. The court balanced the state's need for comprehensive statistical information to enable efficient future planning against the individual's personality right and concluded:

> A possible transmission of data which are neither anonymised nor statistically prepared, i.e. data with personal reference, raises special problems. Surveys for

[260] ibid 120.
[261] ibid 120-121.
[262] ibid at 122.

> statistical purposes embrace individualised information concerning the individual citizen, which is not necessary for statistical purposes but it rather only necessary for the procedure of data collection. All this information can be transmitted according to express statutory authorisations, as long as the transmission serves the purpose of its statistical preparation by another authority and as long as the requirements of the protection of the personality right, in particular the secrecy of the statistics and the commands of an early anonymisation … are guaranteed.[263]

That is, the Court held that the collection of data in the course of a national census was in itself constitutional, as long as the data were only used for statistical purposes, and as long as they were anonymised as early as possible.

iv) Violation of the right to informational self-determination

133. However, the Court held that one provision of the National Census Act, which provided that the personal data to be given on every form could be compared with police registers to see whether the information in those registers was up-to-date, was unconstitutional. The Court held that this use of the information was an unjustified violation of the right to informational self-determination and of Article 2(1), as the information was provided for statistical purposes.[264]

b) Online Computer Surveillance Case

134. The *Online Computer Surveillance Case* is considered to be one of the most important constitutional cases on privacy issues in Germany since the *Census Act Case* in 1983.[265]

i) The nature and purpose of the challenged legislation

135. The Court considered provisions of a North-Rhine Westphalia statute that authorised intelligence authorities to access information technology systems secretly 'through the use of technical means'.[266] The statute did not set out the mode of access that could be used to conduct covert surveillance searches, nor provide for any other substantial or procedural privacy safeguards.[267]

---

[263] ibid 122.
[264] ibid 122-123.
[265] Privacy International (n 244); and Kommers and Miller (n 243) 417.
[266] *Online Computer Surveillance Case* (n 240); G Hornung and C Schnabel (n 242) 116.
[267] ibid.

ii) The nature and scope of the right to the integrity and confidentiality of information technology systems

136. The Court considered that neither the right to secrecy of telecommunications in Article 10 of the German Constitution nor the right to informational self-determination covered the online searching of information technology systems.[268] However, the Court found that this technology was protected under the Constitution by deriving a right to the integrity and confidentiality of information technology systems from the general right of personality in Article 2(1), in conjunction with the guarantee of human dignity in Article 1(1).[269] The Court observed that:

> Today's personal computers can be used for a wide variety of purposes, some for the comprehensive collection and storage of highly personal information … corresponding to the enormous rise in the importance of personal computers for the development of the human personality.[270]

137. In describing the scope of application of this right, the Court held that:

> The fundamental right to the integrity and confidentiality of information technology systems is to be applied … if the empowerment to encroach covers systems that, alone or in their technical networking, contain personal data of the person concerned to such a degree that access to the system facilitates insight into significant parts of the life of a person or indeed provides a revealing picture of his or her personality.[271]

iii) Proportionality assessment

138. The Court did not rule out the possibility of covert searches of computers by intelligence agencies.[272] However, the Court held that such measures may only be justified where established facts indicate that there is an imminent threat to the life, physical integrity or liberty of persons, or to the foundations of the state.[273] In addition, the Court held that covert searches must be subject to judicial oversight.[274] Furthermore, the Court held that the legal basis for such measures

[268] ibid.
[269] *Online Computer Surveillance Case* (n 240); Kommers and Miller (n 123) 417.
[270] ibid.
[271] ibid.
[272] ibid.
[273] ibid.
[274] ibid.

must provide safeguards to prevent any infringements of the 'core of personal privacy'.[275]

iv) Violation of the right to the integrity and confidentiality of information technology systems

139. The Court found that the impugned provisions were incompatible with the implied right to the integrity and confidentiality of information technology systems and unconstitutional, as they did not contain any of these safeguards.[276]

c) Data Stockpiling Case

140. The *Data Stockpiling Case* concerned the largest number of related proceedings ever initiated in the German Federal Constitutional Court.[277] More than 34,000 citizens filed individual actions, supported by the German Working Group on Data Retention *('Arbeitskreis Vorratsdatenspeicherung')*.[278]

i) The nature and purpose of the challenged legislation

141. In the *Data Stockpiling Case*, the Court considered the constitutional validity of amendments to the Telecommunications Act and the Code of Criminal Procedure *('Strafprozessordnung', 'StPO')*.[279] The amendments were enacted to implement European Union Directive 2006/24/EC, which required the mass storage for six months of mobile and fixed-line telephone calls and email traffic.[280] The Directive was aimed at combatting terrorism.[281]

ii) The right to secrecy of telecommunications in Article 10(1)

142. The Court considered that the challenged amendments encroached on the area of protection of Article 10(1) of the Constitution, which guarantees the right to secrecy of telecommunications.[282]

iii) Proportionality assessment

143. In examining the issue of proportionality, the Court held that:

---

[275] G Hornung and C Schnabel (n 242) 117.
[276] *Online Computer Surveillance Case* (n 240); Kommers and Miller (n 240) 417
[277] Privacy International (n 244).
[278] ibid; see also website of the *Arbeitskreis Vorratsdatenspeicherung* (in English) available at <http://www.vorratsdatenspeicherung.de/> accessed 21 February 2013.
[279] *Data Stockpiling Case* (n 124).
[280] ibid.
[281] Kommers and Miller (n 243) 417.
[282] *Data Stockpiling Case* (n 124).

> In view of the particular weight of precautionary storage of telecommunications traffic data, such storage is compatible with [Article 10(1) of the Constitution] only if its formulation satisfies particular constitutional requirements. In this respect, there must be sufficiently sophisticated legislation with well-defined provisions on data security, in order to restrict the use of data, and for transparency and legal protection. … In view of the scope and the potential probative strength of the retained data gathered by such storage, data security is of great importance for the proportionality of the challenged provisions. There is a need for legislation which provides for a particularly high degree of security, whose essential provisions are at all events well-defined and legally binding.[283]

iv) Violation of the right to secrecy of telecommunications in Article 10(1)

144. The Court considered that the retention of such a vast amount of sensitive data would unnecessarily impede the exchange of communication amongst citizens, and were thus incompatible with the right to secrecy of telecommunications guaranteed in Article 10(1).[284]

145. According to the Court:

> [A]n encroachment on liberty interests of such importance … would be compatible with Article 10(1) … only if stockpiling were conducted by private actors for the state's use in investigating criminal acts or preventing security threats, both of which must involve considerable gravity.[285]

[283] German Federal Constitutional Court (*Bundesverfassungsgericht*) Press Office, 'Data retention unconstitutional in its present form' (Press Release No. 11/2010, 2 March 2010) <http://www.bverfg.de/pressemitteilungen/bvg10-011en.html> accessed 21 February 2013.
[284] *Data Stockpiling Case* (n 124); G Hornung and C Schnabel (n 242) 121.
[285] *Data Stockpiling Case* (n 124); Kommers and Miller (n 243) 418.