The handle http://hdl.handle.net/1887/20288 holds various files of this Leiden University dissertation.

Author: Klitou, Demetris
Title: Privacy-invading technologies: safeguarding privacy, liberty & security in the 21st century
Date: 2012-12-14
Criteria for assessing the adequacy of a legal framework in terms of protecting privacy

3.1 CHAPTER INTRODUCTION

It is important to explain what is meant, throughout this dissertation, by an “adequate” or “inadequate” legal framework in terms of protecting privacy, and on what basis, criteria and guidelines, using which methodology, is a legal framework assessed to determine if it is adequate or inadequate.

Section 3.2 introduces the question of what is meant by an adequate privacy legal framework. Section 3.3 introduces the principles of privacy. Section 3.4 explains the purpose and meaning of each privacy principle. Section 3.5 briefly outlines the differences between the European and American approach to safeguarding the right to privacy/data protection. Section 3.6 outlines additional required characteristics for a legal framework to be considered sound. Section 3.7 briefly lists some measures that should be taken before any relevant law is enacted. Section 3.8 outlines some legal criteria specific to the US, while Section 3.9 outlines some specific criteria specific to the UK. Section 3.10 clarifies how the existing privacy principles still apply.

3.2 AN ADEQUATE PRIVACY LEGAL FRAMEWORK?

As a starting point, 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 (hereinafter called “Directive 95/46/EC” or “Data Protection Directive”) provides some guidance on determining adequacy and can help to establish a set of criteria for assessing a legal framework in terms of its adequacy in protecting privacy. The Data Protection Directive requires that EU Member States enact laws prohibiting the transfer of personal data to countries outside the EU that fail to ensure an “adequate level of [privacy] protection”,35 with certain derogations. As provided

---

Criteria for assessing the adequacy of a legal framework in terms of protecting privacy

by Article 25(2), when assessing the “adequacy” of the level of privacy protection in a country the following should be considered or looked at:

- the nature of the data;
- the purpose and duration of the proposed processing operation or operations;
- the rules of law, both general and sectoral, in force; and
- the professional rules and security measures complied with.

But, the Data Protection Directive does not explicitly or necessarily specify the substantive criteria for determining the “adequacy” of the legal frameworks of non-EU countries in terms of privacy protection.

In response, the Article 29 Working Party\(^{36}\) provided further guidance on assessing adequacy in a 1997 document, titled: “First orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy”.\(^{37}\) However, the Article 29 Working Party predominantly dealt with assessing the adequacy of law in terms of information privacy or data protection, which is essentially not broad or comprehensive enough to assess the overall adequacy of privacy/data protection laws with regards to the growing unique challenges posed by many of the latest PITs. Furthermore, the European Commission more recently also expressed their recognition in the important need to “clarify the Commission’s adequacy procedure and better specify the criteria and requirements for assessing the level of data protection in a third country or an international organisation”.\(^{38}\)

---

\(^{36}\) The Article 29 Working Party is a European advisory body on data protection and privacy established under Directive 95/46/EC.

\(^{37}\) Discussion document WP4 (5020/97), First orientations on Transfers of Personal Data to Third Countries — Possible Ways Forward in Assessing Adequacy.

3.3 INTERNATIONAL CONSENSUS IN PRINCIPLE

The principles of privacy/data protection embodied in the Data Protection Directive are clearly based on those previously established by the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) (hereinafter called “OECD Privacy Guidelines”), the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), and the UN General Assembly’s Guidelines for the Regulation of Computerized Personal Data Files (1990). The OECD Privacy Guidelines, in particular, have not only significantly served as the basis of domestic privacy laws in Western democratic nations, but have led to further establishing privacy as a recognized international norm.

There is an international consensus over the fundamental privacy principles and basic rules, which are shared among Western democratic nations and serve as the core substance of privacy and/or data protection laws (Bennett, 1992, p. 95). These fundamental privacy principles recur in some shape or form throughout numerous statutory sources of law, whether domestic, regional or international, ‘hard’ or ‘soft’, and have constituted as the minimum standard of adequate privacy protection. The fundamental privacy principles apply to both the commercial activities of data controllers and the law enforcement activities of public authorities.

The US Federal Trade Commission (FTC) identifies the following as the five core principles of privacy protection:

1. Choice/Consent
2. Access/Participation
3. Notice/Awareness
4. Integrity/Security
5. Enforcement/Redress

While overall the privacy/data protection principles of the FTC, Data Protection Directive (Directive 95/46/EC) and the OECD are similar, the FTC’s set of core prin-

---


40 For further discussion, see Bennett, Colin J. Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Cornell University Press, 1992).

criteria (or Fair Information Practice Principles (FIPPs)) was chosen, since they are arguably more neatly presented and concisely worded. Critically missing, however, from the FTC’s set are (6) the “purpose specification principle”, and (7) the “use limitation principle”, both of which were formulated in the OECD Privacy Guidelines and are significantly applicable to privacy protection in general. In terminology, missing from both sets is the generally accepted legal (8) principle of proportionality.

Similarly, the eight data protection principles, listed in the Data Protection Act 1998 (DPA), which transposes Directive 95/46/EC into UK domestic law, requires that all personal data must be:

1. Processed fairly and lawfully;
2. Obtained and used only for specified and lawful purposes;
3. Adequate and relevant, and not excessive;
4. Accurate and, where necessary, up to date;
5. Kept no longer than necessary;
6. Processed in accordance with the rights of individuals;
7. Secure; and
8. Transferred only to third-party countries that have adequate data protection laws and practices

These data protection principles are parallel to the principles of privacy selected here. The first data protection principle and the conditions that must be met in accordance with Schedules 2 and 3 of the DPA are parallel to the principle of consent/choice. The second data protection principle is parallel to the purpose specification principle and the use limitation principle. The third data protection principle is parallel to the principles of proportionality and data minimization. The fourth data protection principle is parallel to the access/participation principle and the integrity principle. The fifth data protection principle is parallel to the use limitation principle. The sixth data protection principle is parallel to the principles of notice/awareness and consent/choice. The seventh data protection principle is parallel to the principle of security/integrity.

---

42 For instance, the so-called “Bill of Rights” for online privacy, developed with major industry players, is also significantly based on the FIPPs. The FIPPs are rules on the fair treatment of personal data (Schwartz, 2000) and are “the building blocks of modern information privacy law”. (Schwartz, 1999, p. 1614).


44 Ibid., Art. 10.

45 Data Protection Act 1998, Schedule 1, Part I.
Part I

Altogether, the principles of privacy, with the exception of the principle of consent, also serve as the agreed upon principles between the US and EU for a potential binding transatlantic agreement on the exchange of data for law enforcement purposes and the protection of privacy thereof. The principles of privacy also serve as the basis for the EC’s proposal for a new Directive on the processing of personal data for law enforcement purposes.

A wide-ranging and thorough set of criteria permits the clear assessment of the legal adequacy of privacy/data protection laws or lack thereof with regards to the latest PITs. To determine if a legal framework is adequate in terms of protecting privacy and personal data, it should be evaluated against this set of criteria, taking into consideration the intrusive capabilities of PITs (see Chapter 4) on a case-by-case basis.

Throughout this dissertation, the fundamental principles of privacy/data protection will serve, in one way or another, as the criteria and analytical basis for assessing the adequacy of the US and UK legal frameworks/legal practices, with regards to the latest PITs, and for establishing what, if any, amendments, corrections or enhancements to the US and UK legal frameworks are necessary. For the sake of this dissertation, if a legal framework, in its present form, does not fulfill the fundamental privacy principles, where applicable, then it is inadequate (to a certain degree).

3.4 PURPOSE AND MEANING OF EACH PRINCIPLE

The purpose and meaning of each of the interrelated fundamental privacy principles shall correspond to the following:

(1) Choice/Consent

The OECD Privacy Guidelines do not specify exactly what constitutes as consent and how to determine consent. The choice/consent principle is also embodied in the collection limitation principle in the OECD Guidelines.

---

46 see the Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection, May 2008.

47 see Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, Brussels, 25.1.2012.
To determine consent, several aspects should be considered, including whether the consent is informed (see principle (3) notice/awareness), how the consent was obtained by the data controller or granted by the person concerned and whether the consent was somehow forced or if the consent was somehow tied into the permitted exercise of another human right (i.e. indirectly forced). As Article 2 (h) of Directive 95/46/EC requires, consent, in order to be valid, must be “freely given specific and informed”. Moreover, consent must be “unambiguous”. The Article 29 Data Protection Working Party published an opinion further specifying what constitutes valid consent and clarifying the meaning of “freely given”, “specific”, “informed” and “unambiguous”. According to the Article 29 Working Party, “freely given” implies that the consent is a “real choice” and is not based on deception, intimidation, coercion or the threat of significant negative consequences. “Unambiguous” consent implies that there is “no doubt as to the data subject’s intention to deliver consent”.

Directive 95/46/EC also stipulates that a data subject’s consent can be given through any “indication of his wishes”. As the Article 29 Working Party clarifies, “[t]here is in principle no limits as to the form consent can take”. Consent may include not only “a handwritten signature affixed at the bottom of a paper form, but also oral statements to signify agreement, or a behaviour from which consent can be reasonably concluded”. Thus, for the purposes of this dissertation, and in line with Directive 95/46/EC, consent can be validly expressed in written, verbal or electronic form. However, as the Article 29 Working Party also points out, “oral consent may be difficult to prove and, therefore, in practice, data controllers are advised to resort to written consent for evidentiary reasons”. In any case, the express authorization must be recorded or documented.

For the purposes of this dissertation, in line with widely accepted notions, consent shall mean a data subject’s voluntary, informed and expressed authorization to process his/her personal information or to intrude upon his/her privacy, thereby granting the

---

49 Ibid.
50 Ibid., p. 12.
51 Ibid., p. 21.
52 Ibid., p. 11.
53 Ibid.
54 Ibid., p. 25.
person concerned personal autonomy and the freedom to meaningfully choose what he/she would like to reveal about him or herself.

There are certain exceptions to the principle of consent, including when necessary for the protection of public security or for reasons of legitimate public interests, the safety or vital interests of the person concerned (i.e. emergency health concerns), the administration of justice or the prevention or investigation of a criminal offense by competent authorities, in accordance with the law. Consent is also not required when the collection and processing of personal data is deemed necessary to prevent threats to public/national security. Thus, the principle of consent is not applicable for law enforcement operations or surveillance activities, when carried out in accordance with the law, since these activities certainly require secrecy to be effective (Schwartz, 2000). In addition, consent is not required, for obvious reasons, when the processing pertains to personal data that the concerned data subject clearly made public himself/herself (e.g. by publishing it on the Internet via Facebook, Twitter, Blogger, etc.).

With regards to choice/consent, the following are some questions that should be addressed, where applicable:

1. When is consent specifically required and not required?
2. How can consent be expressed? Is the expression of consent recorded/document ed?
3. When is consent considered informed and meaningful?
4. When is consent perceived to be given freely and/or non-freely?
5. Are data subjects permitted to change or withdraw their consent?
6. Is consent required each and every time personal data is collected and processed?
7. What are the consequences of refusing?

(2) Access/Participation

Access and/or participation, for the purposes of this dissertation, shall refer to a data subject’s right of access to the personal data held by data controllers and the capacity or opportunity to review that data and to request that the data be erased or corrected (for instance, where it is evidently determined that the data is inaccurate). Moreover, access/participation encompasses the capacity of data subjects to have removed or the ability

---

to remove themselves any unlawfully retained personal data.\textsuperscript{56} The access/participation principle is referred to as the \textit{individual participation principle} in the OECD Guidelines. The expansion of the access/participation principle could also include the right for data subjects to set their `privacy preferences',\textsuperscript{57} where appropriate, feasible and/or technically possible. However, the principle of access/participation may also be limited for law enforcement purposes or national security interests, albeit in accordance with the law.\textsuperscript{58}

With regards to access/participation, the following are some questions that should be addressed, where applicable:

1. How accessible is the relevant personal data to the person it concerns?
2. How is the right to access and participate granted or implemented?
3. When can a request for access and/or participation be refused?

(3) Notice/Awareness

Notice and/or awareness, as commonly understood, pertains essentially to the requirement of data controllers and/or processors\textsuperscript{59} to clearly and/or visibly communicate, for instance, when personal data could be or is being collected, what sort of information could be or is being collected, how that information could be or is being collected (i.e. using which technology, method or means), why (i.e. for which reason(s)) and by whom (i.e. the identity of the data controller/data processor and often their contact information).\textsuperscript{60} This awareness will also help data subjects to make an informed choice without which the data subject’s consent will not be informed or will be ill-informed. The notice/awareness principle is also based on the \textit{principle of transparency} and is

\textsuperscript{56} see OECD Privacy Guidelines, Explanatory Memorandum, para. 59; Fair Information Practice Principles, available at: http://www.ftc.gov/reports/privacy3/fairinfo.shtm

\textsuperscript{57} Privacy preferences are basically the stipulated circumstances under which a data subject has knowingly given his/her consent for a data controller/data processor to process his/her personal data.


\textsuperscript{59} Article 2 (d) of Directive 95/46/EC defines data controllers as “the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data” and paragraph (e) defines a data processor as “a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller”.

\textsuperscript{60} see OECD Privacy Guidelines, Explanatory Memorandum, para. 57; Fair Information Practice Principles, available at: http://www.ftc.gov/reports/privacy3/fairinfo.shtm
essentially the same as the openness principle found in the OECD Privacy Guidelines. Nonetheless, there are also certain exceptions to the notice and/or awareness principle when the exceptions are proportionate and necessary for law enforcement purposes, in accordance with the law, or necessary for competent authorities to execute their legitimate responsibilities.\(^{61}\)

With regards to notice/awareness, the following are some questions that should be addressed, where applicable:

1. In what form should the notice be communicated?
2. Where is the notice communicated?
3. What is exactly communicated?
4. Who is primarily responsible for ensuring the notice is appropriately visible?

(4) Integrity/Security

The security of personal data and of the infrastructure storing that information is at the heart of privacy. Without data security, there can be no data protection/privacy. The security of personal data often corresponds to the requirement of data controllers to take the necessary technical and organizational measures to safeguard against any unlawful or unauthorized access, use, modification or disclosure of any personal data that they are storing.\(^{62}\) Data security is, therefore, also essential for data integrity and the data quality principle of the OECD Privacy Guidelines, which corresponds to the notion of data accuracy, relevance and reliability.\(^{63}\)

With regards to data integrity/security, the following are some questions that should be addressed, where applicable:

1. What measures must be taken to ensure the integrity and security of personal data?

---


\(^{63}\) The original FIPs, established by the US Department of Health, Education and Welfare, included data “reliability”, and the recent Department of Commerce, Internet Policy Task Force Green Paper, “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework” (2010), affirmed that organizations must ensure that stored personal information is “accurate, relevant, timely, and complete” (p. 26).
2. If possible, how can data controllers and data subjects ensure that these measures have been implemented or realized?

3. Are these measures mandated in accordance with binding hard laws/regulations or encouraged through soft laws/voluntary standards/codes of conduct?

(5) Enforcement/Redress

Although the privacy principles are inter-dependent and each is equally fundamental, like integrity/security, enforcement is crucial. The principles are only genuinely effective to the extent and scope in which they are complied with, implemented or followed in practice. Both the privacy principles and the laws that embody the principles cannot enforce or implement themselves on their own. Essentially, without the means of enforcement, the privacy principles could end up ineffective or even ignored. It is, therefore, necessary to consider not only the content of the law, but also the means of enforcement or the enforcement mechanisms that are in place to ensure the laws have a genuine effect and impact.

Enforcement, for the purposes of this dissertation, entails the impartial means to oversee and verify compliance and investigate and resolve complaints. Accordingly, the principle of enforcement requires independent and effective oversight/supervision. Enforcement also includes the availability of both non-judicial (or administrative) means to provide appropriate redress and judicial means to penalize the responsible parties who violate the right to privacy. Arguably, victims of privacy violations should also have the right to receive damage awards, where deemed appropriate by a court of law. Criminal sanctions should be mandated for serious violations. Arguably, enforcement should always entail the right to private legal action before an impartial and independent tribunal.

The accountability principle of the OECD Privacy Guidelines relies on the principle of enforcement/redress, but both principles are not the same. Accountability is more focused on assigning liability to the responsible entities/authorities for ensuring the protection of privacy and is more emphasized “on showing how responsibility is exercised and making this verifiable”\textsuperscript{64}, i.e. requiring data controllers to implement measures for upholding the data protection principles and to demonstrate that the measures taken are both appropriate and effective.\textsuperscript{65}


\textsuperscript{65} Ibid.
Both enforcement and accountability require the identification of the responsible entities/authorities, which are primarily, at present, the relevant data controllers and/or processors. According to the OECD Privacy Guidelines, similar to Directive 95/46/EC, data controllers are the responsible entities or persons “competent to decide about the contents and use of personal data”. However, identifying the responsible data controllers is not always easy, especially as a result of the increase in cross-border data flows and the complexity of information systems. Moreover, while the existence, nature and content of enforcement mechanisms can be assessed, “[t]he assessment of adequacy will be incomplete to the extent that it cannot assess actual practices and the realities of compliance”.66

With regards to enforcement/redress and accountability, the following are some questions that should be addressed, where applicable:

1. What enforcement mechanisms are available?
2. If available, what are the specific legal sources that establish the enforcement mechanisms?
3. Are both judicial and non-judicial remedies available for data subjects?
4. Is the right to private legal action available?
5. Can data controllers be held criminally liable for serious privacy violations? Are they also subject to civil action and penalties?
6. Can the injured data subjects be rewarded monetary compensation for these violations? Are the criminal sanctions and monetary sanctions sufficiently rigorous to ensure compliance?
7. Is there a supervisory public authority responsible for overseeing compliance? What are the enforcement powers of this supervisory public authority and how independent or impartial is it?

(6) Purpose Specification

The purpose specification principle requires that the purposes for which personal data is lawfully collected must be transparent and specified beforehand (usually in writing), and its subsequent processing (collection, use, retention, modification, analysis, distribution, etc.) must be limited to the fulfillment of those specific purposes and not

contrary to them. The purpose specification principle also holds that personal data should not be retained for longer than necessary to fulfill those purposes. Once its retention is no longer necessary to fulfill the specified purpose for which it was collected, data controllers must then delete or destroy the relevant personal data or, at minimum, unequivocally anonymize the personal data. 67 The principle is considered essential since “informed consent to the collection and processing of his/her personal data is dependent on the information about the purpose and use of those data” (Tzanou, 2010, p. 421). The purpose specification principle, for instance, is embodied in Article 6.1(b) of the EU’s Data Protection Directive (Directive 95/46/EC).

With regards to purpose specification, the following are some questions that should be addressed, where applicable:

1. What are data subjects informed concerning the purpose of the data collection?
2. Are there any legally binding restrictions on the purposes for which personal data can be collected?
3. How is it determined that personal data is no longer needed to fulfill the specified purpose for which it was collected?

(7) Use Limitation

The use limitation principle requires that personal data should not be used in any way beyond the originally stated objectives for which it was collected, unless with the explicit consent of the concerned data subject or explicitly permitted by law. The use limitation principle helps to prevent “function creep”. Function creep occurs when “personal data collected for one specific purpose and in order to fulfill one function, are used for completely different purposes, which are totally unrelated to the ones for which they were initially collected”. 68

With regards to use limitation, the following are some questions that should be addressed, where applicable:

1. When are the originally stated objectives deemed to have been achieved?
2. How can data subjects be sure that their personal data is not used beyond what they have been informed of and have originally consented to?

67 see OECD Privacy Guidelines, Explanatory Memorandum, para. 54.
(8) Proportionality

The principle of proportionality is a general legal principle often used in both domestic criminal law, to represent the notion that the punishment for a criminal offense must be relative to its gravity, and in international law, to regulate a state’s use of armed force during a conflict, whereby the harm brought upon civilians and civilian infrastructure must be relative to the intended lawful and specific military objectives sought after.

The legal principle of proportionality also effectively applies to privacy/data protection law. As widely recognized, the legal principle represents the notion that the processing (collection, use, retention, modification, analysis, distribution, etc.) of personal data and/or the infringement upon privacy, whether based on consent or not, should be necessary, reasonable, appropriate, relevant and not excessive in relation to the specific, legitimate purpose(s)/aim(s) for doing so (e.g. security gains), in accordance with the law in a free and democratic society. The principle of proportionality is applicable, regardless of the purported legitimate purpose(s)/aim(s) sought after. In addition, as widely understood, the principle of proportionality also applies to the chosen means/measures (i.e. method, technology, etc.) used. If less intrusive or more reasonable means/measures are available to equally achieve the same legitimate aim(s), then those means should arguably be chosen instead. Accordingly, both the relevance of the purported legitimate aim(s) and the factual circumstances and consequences of the employed means must be considered (for further discussion, see, e.g., Taylor, 2002a).

Specifically, in terms of data protection, the principle of proportionality is also connected with the data minimization principle and the collection limitation principle, which collectively require that no more data should be collected than is required for the specified purpose(s)/aim(s) of its collection and that the personal data should only be obtained through lawful means.

---

69 see, e.g., Charter of Fundamental Rights of the European Union, Article 52(1).
3.5 THE EUROPEAN APPROACH VS. THE AMERICAN APPROACH

Again, there is indeed consensus among Western free and democratic nations over the fundamental principles of privacy, but there are differences of opinion, particularly between policy makers/lawmakers in the EU and the US, over how to best implement the fundamental principles and what the machinery of enforcement and redress should entail. These differences, some of which were previously highlighted by Bennett (1992) and Reidenberg (2000), are still valid.

Among EU Member States, there is somewhat broad agreement that privacy principles and data protection rules must be codified in legally-binding legislation and backed by an independent, dedicated, central/national and governmental supervisory agency with the authority to investigate complaints, ensure compliance and impose sanctions for non-compliance. This agreement was manifested in the adoption of Directive 95/46/EC – a comprehensive, broad, multi-sectoral privacy legislation that regulates practically all data collection/processing activities, regardless of the technology concerned, of both private entities and public authorities (except for law enforcement agencies). The EU’s regulatory approach is thus technology-independent. Accordingly, each EU Member State has passed domestic legislation transposing Directive 95/46/EC and has established a national data protection supervisory authority. As Reidenberg (2000) points out, although there are varying legal interpretations of Directive 95/46/EC within the EU, there is clearly a “common view that data protection is a basic human right that must be guaranteed by the state”. The European legal approach has had a direct influence on the legal frameworks of other countries outside the EU, such as Australia, New Zealand, Japan, South Africa and Canada (Birnhack, 2008).

Nevertheless, while legally binding ‘hard’ laws are customary for protecting privacy in Europe, self-regulations (or non-legally binding ‘soft’ laws) are also occasionally relied upon.

---

70 The current negotiations between the US and EU over a future binding transatlantic agreement on the exchange of data for law enforcement purposes and the protection of privacy thereof may highlight these differences.

71 For further discussion, see Bennett, Colin. Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Cornell University Press, 1992).

72 Birnhack, Michael D. The EU Data Protection Directive: An Engine of a Global Regime (Tel Aviv University Law Faculty Papers, Paper 95, 2008).

The US legal approach to protecting privacy is based instead on a unique mixture of separate statutory laws for various subject matters/technologies/domains, case law and self-regulations. In particular, the US approach is sectoral rather than all-inclusive or comprehensive, which is partly the cause for some of the deficiencies or gaps in the US legal framework, as explained in the subsequent chapters of the dissertation. The US regulatory approach is thus technology-dependent. Moreover, the US Congress often passes laws only after a serious problem or incident arises and not before. As Reidenberg (2000) similarly points out, under the US approach, the “law only intervenes on a narrowly targeted basis to solve specific issues where the marketplace is perceived to have failed”. Still, the US has not successfully passed legislation similar to the EU’s Directive 95/46/EC. The Privacy Act of 1974, for instance, is nowhere near as comprehensive and broad as Directive 95/46/EC and nor does it apply to private entities. While there are other specific privacy protection laws for different subject matters, domains or technologies, voluntarily adopted self-regulations/industry codes of conduct/corporate practices are instead primarily relied upon, at present, to safeguard privacy in the US (Reidenberg, 2000). Data controllers are free to formulate these regulations and are primarily responsible for ensuring their compliance.

However, although in the US there is no dedicated, governmental supervisory authority, equivalent to the national data protection supervisory authorities in EU Member States, to enforce compliance with privacy rules, the enforcement of corporate self-regulations/privacy policies are supervised by the FTC. The FTC has the authority to act against unfair and deceptive practices or broken promises. While the FTC is the closest body in the US to a national data protection supervisory authority, there is also in the US the Privacy & Civil Liberties Oversight Board. There are also offices of privacy protection on the state-level, but the responsibilities of these bodies are merely advisory.

On the other hand, as Bignami empirically reveals, tort litigation for privacy violations in the EU still plays a relatively insignificant role compared to within the US. Instead, administrative redress plays a more significant role in the EU. However, as Bignami also reveals, the number of tort litigation cases for privacy violations in the EU has

---

"The Privacy and Civil Liberties Oversight Board (PCLOB) was established after the National Commission on Terrorist Attacks Upon the United States (known as the 9/11 Commission) recommended it. The PCLOB is an independent agency within the executive branch and is meant to provide oversight in the fight against terrorism. But, the PCLOB is still inactive."
steadily increased since the adoption and transposition of Directive 95/46/EC,\textsuperscript{75} which provides for judicial remedy and the awarding of compensation for privacy violations.\textsuperscript{76}

In accordance with the OECD Privacy Guidelines, however, there is essentially no single, correct way of enforcing or implementing the privacy principles, as long as they are indeed enforced or implemented in practice. In actual fact, the OECD Privacy Guidelines explicitly “permits Member countries to exercise their discretion with respect to the degree of stringency with which the [OECD Privacy] Guidelines are to be implemented, and with respect to the scope of the measures to be taken”,\textsuperscript{77} and does “not presuppose their uniform implementation by Member countries with respect to details”.\textsuperscript{78}

In spite of this, for the sake of this dissertation, the assessment of the adequacy of enforcement/redress mechanisms is, for the most part, based on the European approach.

\textbf{3.6 REQUIRED LEGAL CHARACTERISTICS}

In parallel with the application of the fundamental privacy principles, there are other legal characteristics that should arguably be considered when assessing the adequacy and soundness of a legal framework in terms of privacy protection. Based on these required legal characteristics, other legal deficiencies and dilemmas in the legal framework can also be determined.

In terms of ensuring the protection of privacy, the legal framework should also be:

- Legally binding, ‘hard’, actionable and enforceable;
- Consistent;\textsuperscript{79}
- Precise, clear\textsuperscript{80} and not ambiguous.\textsuperscript{81}

\textsuperscript{75} Prof. Francesca Bignami presented her empirical analysis at the third annual international conference Computers, Privacy and Data Protection (January 29-30 2010, Brussels), which I attended. see Bignami, Francesca. The Non-Americanization of European Regulatory Styles: Data Privacy Regulation in France, Germany, Italy, and Britain (Center for European Studies Working Paper Series #174, 2010), available at: http://www.ces.fas.harvard.edu/publications/docs/pdfs/CES_174.pdf
\textsuperscript{76} see Articles 22 and 23 of Directive 95/46/EC.
\textsuperscript{77} OECD Privacy Guidelines, Memorandum, para. 45.
\textsuperscript{78} Ibid.
\textsuperscript{79} see Tamanaha, Brian Z. On the Rule of Law: History, Politics, Theory (Cambridge University, 2004).
\textsuperscript{80} see, e.g., Khan v. United Kingdom, Application no. 35394/97, Judgment of 12 May 2000, §26.
\textsuperscript{81} see Tamanaha, Brian Z. On the Rule of Law: History, Politics, Theory (Cambridge University, 2004).
Part I

- Free of vague concepts and/or definitions;
- Free of legal loopholes;
- Foreseeable (the law should be of such quality and precision that determining when it has been complied with or breached is apparent and predictable, and if breaches are permitted, then the justification for doing so must also be precise and clear).\(^{82}\)
- Readily accessible,\(^{83}\)
- Flexible, but also specific, where and when needed;
- Up to date with current PITs and anticipatory of their further advancement;
- Not primarily dependent on self-regulations, whether governmental or private;
- Not primarily dependent on case law;
- In compliance with relevant international norms and other legal instruments; and
- Not completely contrary to the recommendations of international organizations, such as the OECD, United Nations and Council of Europe, or perhaps the domestic laws of other countries widely considered democratic and free.\(^{84}\)

If any legal framework or legal practice is contrary to or lacks any of these required legal characteristics, where applicable, then the law may be inadequate, to a certain extent or degree, depending on the extent and scope of the contradiction and deficiency.

3.7 BASIC PRE-MEASURES

In addition, based on both common practices and the privacy principles, other basic measures should arguably be carried out before any relevant law is enacted, policy adopted, policy instrument implemented or PIT deployed. These basic pre-measures may include:

- An assessment of the impact upon privacy;
- Identification and testing of possible alternative means for achieving the same end in a less intrusive manner; and
- Public engagement with relevant stakeholders, requesting public input/comments, and taking into account the concerns of the general public.


\(^{83}\) Ibid.

\(^{84}\) Of course, what makes a country “democratic and free” is a whole other question, which requires its own set of criteria.
3.8 LEGAL CRITERIA SPECIFIC TO THE US

In the US, the law must be capable of upholding the integrity of the US Constitution, in particular the freedom from unreasonable search and seizure enshrined in the Fourth Amendment. Where applicable, the law must comply with the Privacy Act of 1974 and other relevant statutory laws, both federal and state.

3.9 LEGAL CRITERIA SPECIFIC TO THE UK

In the UK, the law must be capable of upholding the right to a private life, as enshrined in Article 8 of the European Convention on Human Rights (ECHR) and incorporated into domestic law through the Human Rights Act (1998). The law should comply with judgments of the European Court of Human Rights (ECtHR). All UK laws must comply with the principles enshrined in the Data Protection Directive and the Data Protection Act (1998), which incorporates the EU Directive into UK law. Moreover, UK lawmakers should equally take into consideration the recommendations and opinions of the Council of the EU, the European Commission, the Council of Europe, the Article 29 Working Party and the European Union Agency for Fundamental Rights.

3.10 APPLYING THE PRIVACY PRINCIPLES OF THE 20TH CENTURY TO THE TECHNOLOGICAL ADVANCEMENT OF THE 21ST CENTURY

As reaffirmed by OECD member states, during a 1998 conference in Ottawa, Canada and declared in a Ministerial Declaration on the Protection of Privacy on Global Networks:

the technology-neutral principles of the 1980 OECD [Privacy] Guidelines continue to represent international consensus and guidance concerning the collection and handling of personal data in any medium, and provide a foundation for privacy protection on global networks.85

Indeed, however, the OECD Privacy Guidelines “were prepared in the context of the technology then known and envisaged,” as the Hon Justice Michael Kirby, who chaired the expert group that produced the OECD Privacy Guidelines from 1978-80,

85 Organisation for Economic Co-operation and Development, Ministerial Declaration on the Protection of Privacy on Global Networks, Ottawa, 7-9 October 1998, DSTI/ICCP/REG(98)10/FINAL.
pointed out.\textsuperscript{86} While the velocity and scope of the advancement of PITs since 1980 has been remarkable, the fundamental privacy principles formulated by the OECD can potentially still meet the technological challenges of the 21\textsuperscript{st} Century and still remain applicable “irrespective of the particular technology employed”.\textsuperscript{87} However, the endless advancement and deployment of PITs equally requires new and specific guidance on how to apply the privacy/data protection principles in practice,\textsuperscript{88} and may require further legislative and non-legislative action to ensure their effective application.\textsuperscript{89}

Moreover, perhaps contrary to the OECD’s earlier view, some of the principles, particularly the \textit{use limitation} and \textit{purpose specification} principles (in addition to the \textit{principle of proportionality}), are not only applicable to the processing of personal information/data, but also to the protection of privacy in general. For the most part, the privacy principles can also potentially be adapted to address privacy violations no matter where and in which manner they occur. The continued relevance of the fundamental privacy principles is demonstrated by the case studies.

PART II (Chapters 5, 6, 7) evaluates/assesses the adequacy of the legal frameworks in the US and UK, based on the criteria outlined in this chapter, in light of the privacy-intrusive capabilities of the following four particular PITs: body scanners; CCTV microphones and loudspeakers; and human-implantable microchips (RFID implants; GPS implants).


\textsuperscript{87} OECD Privacy Guidelines, Explanatory Memorandum, para. 37.


\textsuperscript{89} see COM (2009) 262 final, Communication from the Commission to the European Parliament and the Council - An area of freedom, security and justice serving the citizen.